法律家から見た個人情報漏洩問題

弁護士
尾崎　孝良

かつては、インターネットセキュリティ関連のインシデントといえば、ウイルス、不正アクセス・侵入、ハッキング・クラッキングというのが定番であった。しかし、昨今のセキュリティのインシデントといえば、個人情報の流出事故であり、しかも朝日新聞がまとめた「企業の個人情報の主な流出・紛失例」をみると

時期		企業名	規模
03年	6月	ローソン	56万人
	8月	アプラス	8万人
	10月	ファミリーマート	18万人
04年	1月	三洋信販	116万人
	2月	ソフトバンクBB	451万人
		シティバンク	12万人
	3月	ジャパネットたかた	30万人
		アッカ･ネットワークス	30万人
		東武鉄道	13万2000人
		サントリー	7万5000人
	4月	コスモ石油	92万人
		日本信販	10万人
	5月	三菱マテリアル	1000人
		ツノダ	3000人
	6月	阪急交通社	62万人
		良品計画	1124人
		Bs-i･P&G	1万人

（出典：http://www.asahi.com/special/privacy/index.html）

2004年前半だけですでに十数件の事故が発生し、各事件で数千人～数百万人までの個人情報が流出している。

中でも、500万人近く（最近の報道では実は660万人分だったともされている）の情報を流失してしまったYahoo! BB事件が最も深刻である。

■Yahoo! BB事件---470万件流出

本年2月24日ころ報道各紙に「Yahoo! BBから470万人分の個人情報が流出」との見出しが踊った。

当初、ソフトバンク側は「それら（470万件）がYahoo! BBユーザーのデータであるかどうかは確認していない」（宮内副社長）と述べ、同月25日から照合作業を開始した。

そして、同月27日、ソフトバンクは、警察から提供を受けたデータの照合結果について発表、451万7千件の個人情報が流出していたことを明らかにした。同社の孫正義社長は陳謝するとともに、Yahoo!BBのすべてのユーザに対し、500円相当の金券などを送るとした。

3月18日には、管理諮問委員会名で、報告書が発表された。その内容は以下のとおり。

・「正規アクセス権者からパスワードを漏らされた者」の侵入ではなく「正規アクセス正規パスワードによる犯罪目的利用」ではないかと結論づけた（なお、この点について、後に退職した者がパスワードを漏洩したことが判明）。

・データベースへアクセスするには、ID・パスワードを使う仕組みとなっており、ID・パスワードは、情報管理の担当者が、現場担当者からの請求に応じて、必要に応じる形で発行していた。2003年7月以降のパスワードは、4箇所のデータベースのいずれかにアクセスできるという意味でのアカウントを総計した場合に、135件発行されていた事実が報告され、内数件はグループ・アカウントとして発行されていたとのことであった。

・パスワードの管理方法については、セキュリティに関する注意規定が作成、公表されており、特にその中に「IDとパスワードの管理について」との文書が作成されており、管理教育が行われており、通常のパスワード管理体制は確立されており、ずさんな管理を行っていたとまではいえないと結論づけた。

・以上を前提に、顧客に対する500円のお詫び料の支払については、「相当な範囲にある」とした。

■ずさんな管理体制

ところが、5月30日ころになって、情報を漏洩した者とその協力者が判明。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者（協力者）が、ソフトバンクBB株式会社のリモートメンテナンスサーバへアクセスするためのアカウントとパスワードを容疑者らに伝え、容疑者らは同サーバを経由して顧客データベースへ不正にアクセスし、顧客情報を持ち出したことが判明した。

協力者は2002年5月から2003年2月まで、ソフトバンクBB株式会社サービスオペレーション本部にて業務委託者として、ネットワークメンテナンスやサーバ構築業務に従事してた、という。協力者は業務における必要性から、リモートメンテナンスサーバへのアクセス権限を保有していた。また、顧客データベースへのアクセス権保有者170名（135アカウント）の中の1名。

つまり、既に退職していたにもかかわらず、IDパスをそのまま放置していた実態が明らかになったのだ。

さらに、6月18日なると、「（同容疑者が）同社のIP電話「BBフォン」の通話記録も引き出していたことが警視庁の調べでわかった。また、同容疑者が引き出したヤフーBBの顧客情報は、今年1月時点の登録者全員にあたる約660万人だったという。同社の情報管理のずさんさが改めて浮き彫りになった」（朝日新聞）と報道された。

以上のように、Yahoo! BB事件は、セキュリティ意識の甘い企業体質が通信記録といった極めてプライバシー性の高い情報を流出するという事態にまで発展してしまった事例である。

■個人情報保護法の概説

このような大事件が発生する中で法律の仕組みははどのようになっているのか。まず、最近各所で話題の個人情報保護法の内容についてみてみよう。

個人情報保護法は、昨年5月に成立し、来年4月の本格施行に向けて、関係省庁がガイドラインなどを策定しているところである。

この法律の目的は、「個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の有用性に配慮しつつ、個人の権利利益を保護すること」（第1条）としている。

なお、インターネットではよく「この法律は、個人情報利用の有用性に配慮しつつも、個人のプライバシーに関する権利を保護していくことを目的にしている」との表現をみかけるが、誤りである。プライバシーと個人情報は（密接に関連するが）概念が異なる。

この法律における「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。）」（2条1項）をいう。特定の個人を識別することができれば、公開情報であっても個人情報となる。たとえば名刺に記載されているような事項は（プライバシー情報とはなり得ないが）個人情報だ。

そして、「個人情報を含む情報の集合物」であって「電子計算機を用いて検索することができるように体系的に構成したもの」等を「個人情報データベース等」という（同条2項）

この「個人情報データベース等」を事業の用に供している者が、個人情報取扱事業者であり、主として個人情報取扱事業者がこの法律の各種規制を受けることになる。なお、「個人情報データベース等」を事業の用に供している者であっても、国の機関や公共団体は対象にならないし、また、「その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定める者」も除外されることになる。

これを受けて、政令2条で「法第二条第三項第四号の政令で定める者は、その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定

の個人の数の合計が過去6か月以内のいずれの日においても五千を超えない者」と規定した。したがって、過去6か月のうち、1日でもDB上の個人情報が5000件を超えてしまったら、個人情報取扱事業者となってしまうので注意が必要だ。

なお、法律相談や講演会の質疑でよく聞かれるのだが、①上記施行令2条の内容と、②法2条5項（その具体的内容は施行令4条で規定）で規定される「6か月以内に消去すれば同法上の保有個人データに該当しない」との例外規定とを混乱している方が多いようなのでここで注意を喚起しておく。すなわち、個人データを6か月以内に消去したとしても、ある1日のデータ量が5000件を超えていれば、個人情報取扱事業者となる（ただし、規制の多くは、「保有個人データ」を客体とするので、データを全部6か月以内に消去していれば法的規制をほとんど受けないといえる。上記法令を勘違いして、5000件を若干上回るデータを有している企業が、6か月以内にわずかな数を消して5000件を超えないようしても、当該企業は個人情報取扱事業者であり、その企業の保有する個人データについては個人情報保護法の規制対象となる）。

限られた企業のみとしか取引しない零細子会社以外、ほとんどの企業が規制対象となると考えてよい。

■個人情報取扱事業者の責務（OECD 8 原則に照らして）

個人情報を取得した個人情報取扱事業者は、取得・利用・管理のすべてのプロセスにおいて責任を負うことになる。

情報主体である個人の許可なしに、表示した目的以外の使用や、第三者への提供をしてはならない。また、個人情報取扱事業者は、管理体制を整備し、実施することが求められる。

個人情報取扱事業者に課せられる、主な義務をまとめてみよう。

個人情報保護の基本原則として、OECD（経済協力開発機構）が1980年9月23日「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」（Recommendation of the Council concerning Governing the Protection of Privacy and Transborder Flows of Personal Data）としてまとめた、OECD 8 原則

①収集制限の原則（Collection Limitation Principle）
②データ内容の原則（Data Quality Principle）
③目的明確化の原則（purpose Specification Principle）
④利用制限の原則（Use Limitation Principle）
⑤安全保護の原則（Security Safeguards Principle）
⑥公開の原則（Openness Principle）
⑦個人参加の原則（Individual Participation Principle）
⑧責任の原則（Accountability Principle）

が国際的な基本原則となっている。個人情報保護法の政府の提案趣旨もこのOECD 8 原則に対応する形式で整理されているので、以下、趣旨説明資料（第156回国会）から引用しよう。

○ 目的明確化の原則
収集目的を明確にし、データ利用は収集目的に合致するべき

○ 利用制限の原則
データ主体の同意がある場合、法律の規定による場合以外は目的以外に利用使用してはならない

- 利用目的をできる限り特定しなければならない。（第15 条）
- 利用目的の達成に必要な範囲を超えて取り扱ってはならない。（第16 条）
- 本人の同意を得ずに第三者に提供してはならない。（第23 条）

○ 収集制限の原則
適法・公正な手段により、かつ情報主体に通知又は同意を得て収集されるべき

- 偽りその他不正の手段により取得してはならない。（第17 条）

○ データ内容の原則
利用目的に沿ったもので、かつ、正確、完全、最新であるべき

・ 正確かつ最新の内容に保つよう努めなければならない。（第19 条）

○ 安全保護の原則

合理的安全保護措置により、紛失・破壊・使用・修正・開示等から保護するべき

・ 安全管理のために必要な措置を講じなければならない。（第20 条）
・ 従業者・委託先に対し必要な監督を行わなければならない。（第21 、22 条）

○ 公開の原則

データ収集の実施方針等を公開し、データの存在、利用目的、管理者等を明示するべき

○ 個人参加の原則

自己に関するデータの所在及び内容を確認させ、又は意義申立を保証するべき

・ 取得したときは利用目的を通知又は公表しなければならない。（第18 条）
・ 利用目的等を本人の知り得る状態に置かなければならない。（第24 条）
・ 本人の求めに応じて保有個人データを開示しなければならない。（第25 条）
・ 本人の求めに応じて訂正等を行わなければならない。（第26 条）
・ 本人の求めに応じて利用停止等を行わなければならない。（第27 条）

○ 責任の原則

管理者は諸原則実施の責任を有する

・ 苦情の適切かつ迅速な処理に努めなければならない。（第31 条）

■罰則と行政指導法の限界

個人情報保護法の罰則についてみると、個人情報取扱事業者の違反行為には、最終的には、罰金などの罰則が科されることになる。違法行為是正の仕組みは以下のとおりだ。

まず、個人情報取扱事業者が上記各条の規定に違反した場合には、個人の権利利益を保護するため必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を、主務大臣が「勧告」することができる（34条1項）。

そして、この勧告を受けた個人情報取扱事業者が正当な理由がなくてその勧告に係る措置をとらなかった場合において個人の重大な権利利益の侵害が切迫していると認めるときは、当該個人情報取扱事業者に対し、その勧告に係る措置をとるべく「命令」を発することになる（同条2項）。なお、緊急の場合は、1項の勧告をせずに命令を先行できる（同条3項）。

そしてこれらの「命令（34条2項又は3項）」に違反した者は、6か月以下の懲役又は30万円以下の罰金が科せられる（56条）。法人の役員や従業員が違反した場合は、両罰規定により法人にも罰金が科せられる（58条1項）

■情報漏洩に関する刑事法制

以上みたとおり、個人情報保護法というのは、法律の規定する「個人情報」（これは必ずしも知られたくないプライバシー情報とは限らない）を事業者が管理すべく、監督官庁が指導する行政指導法であって、この法律に基づいて企業が個人に損害賠償責任を負うことはない。

もちろん、法律の「理念」は、前述のとおり、OECDの8原則に準拠した妥当な内容となっているのだが、あくまで行政指導法であって、各個人に個人情報事業者に対する新たな権利を付与したものではない。

また、勧告→命令という手続きを経て悪質な命令違反がある場合には刑罰が科されることになるが、通常はそこまでいく前に、監督官庁の指導に服するだろう。

では、個人情報が流出したり、不正に利用された場合、それらの行為に対する罰則はあるのだろうか？

他人の情報を無断で盗み見ることは悪いことだというのは常識だろう。特に、他人に知られたくないプライバシー情報を勝手に入手してはいけない、誰もがそう思う

だろう。

しかし、社会常識とか道徳に照らして「悪いこと」がすべて「犯罪」として処罰されるかというとそうではない。

情報を勝手に「盗む」のだから単純に泥棒（窃盗罪）なのでは？と考える方も多いのだが、そう簡単ではない。

刑法235条窃盗罪の構成要件は、他人の占有する「財物」を不法領得の意図をもって自己の占有に移すことである。

ここで「財物」というのは有体物（形あるもの）のことをいう。唯一の例外は、電気エネルギーだ（刑法245条）。したがって、「情報」のような無体物は「財物」でない。情報窃盗は窃盗罪ではないのである。

話はそれるが、利益（債権）も財物ではないから、利益の窃盗も犯罪ではない。たとえば、レストランで最初はお金を払うつもりで注文し（最初から食い逃げするつもりだと詐欺罪になる）、レジのとこまで行ったらサイフが無いのに気づいて走って逃げた、という事案は、典型的な「利益窃盗」で刑法上の窃盗罪には該当しない（警察は、窃盗容疑で逮捕することはできない）。むろん、道義的には許されることではないので、決しておすすめはしないが。

企業内の情報が盗まれた場合、フロッピーやCD-R、印字した紙が企業の占有物であった場合、盗まれた財物に注目して窃盗罪として立件するのが実務的な運用である。情報を盗むこと自体は犯罪事実ではなく、企業の占有下にあるフロッピーとか紙という「財物」（ずいぶん安い「財物」ではあるが）を自己（犯人）の占有に移した事実をもって窃盗罪としている。そのフロッピーに重要な情報が入っていたというのは、情状（罪の重さを決める事情）となる。

したがって、メールやファイル転送を利用して情報を漏洩した場合、刑法犯にはなり難い。極端な話、情報を丸暗記して持ち出してしまえば、それがどんなに重要な情報であろうと犯罪扱いされることはない。

これだけ、情報が大きな価値を持つ時代になってしまったのに、法律が時代に追いついていないともいえる。

このようなコンテクストから、「新しくできた個人情報保護法というのは情報窃盗を取り締まる法規である」と勘違いする向きもあるようだ。このような解説をインターネット上での掲示板などで散見する。しかし、個人情報保護法は、後述するとおり、「個人情報取扱事業者」に課せられる事業者規制法である。刑法の窃盗犯の特別法ではない。おそらく、「情報の窃盗は取り締まることができない」という立法背景を読み違えた理解と思われる。

それでは、「刑法を改正して、情報も財物とすれば良いではないか」と考える方もいると思うが、事はそう簡単ではない。安易に情報窃盗を窃盗罪にすると、本屋の立ち読みなども該当してしまう。日常生活で無償で情報をもらう場面は意外と多いのだ。また、財物と異なり「占有」の認定が難しいので、いつ窃取したのかの認定も困難だ。

カメラ付き携帯電話の普及で、本屋で必要な情報を撮影するのが法的にどのように評価されるのか（刑法の立法論のほかに著作権法上の問題もある）、まだまだ議論の尽きないところであり、立法化は容易でない。

■贈収賄罪等の可能性

窃盗罪に該当しなくとも、他の罪に問われることがある。よくある類型は贈収賄だ。国家公務員やNTTなどの特殊法人が業務データを提供する見返りとして、金銭を受け取った場合収賄罪になる（金銭を渡した側は贈賄罪）。

ただし、民間企業同士ならどんなリベートを渡そうが贈収賄にはならない。

また、地方自治体では、個人情報保護条例を定めているところもある。後述の宇治市事件では、市の「電算組織に係る個人情報の保護に関する条例」に違反するとして、データを持ち出した外部委託業者を刑事犯として告訴した（ただし、特殊事情により不起訴処分となった。後述）。

要するに（NTTのような特殊法人を除く）民間企業から個人情報が漏洩しても刑事事件として立件することは

難しい。結果として、情報を漏らした者に対する制裁が十分できない。告訴すらできないという事態も考えられる。管理の甘かった企業に対する社会的な批判が集中する。その企業は、何ら事後対策をすることもできず信用を失うということになってしまうのが実態だ。

■不正競争防止法

以上のとおり、一般の企業や個人が秘密を漏洩しても何ら罰則規定も存しなかったのであるが、平成１６年１月から改正不正競争防止法が施行された。

改正法では、営業秘密の侵害に対する刑事罰の導入などが盛り込まれている。

例えば、同法14条１項３号では、詐欺等行為や管理侵害行為（営業秘密が記載され、又は記録された書面又は記録媒体の窃取、営業秘密が管理されている施設への侵入、不正アクセス行為その他の保有者の管理を害する行為）により取得した営業秘密を、不正の競争の目的で、使用し、又は開示した者は、３年以下の懲役又は300万円以下の罰金が科されると規定している。

これによって、従来不可罰であった「情報窃盗」の一部が、営業秘密に限り罰せられる可能性が出てきた。

■情報窃盗罪立法化の危険

本年５月12日に日経新聞が「産業構造審議会（経産相の諮問機関）の情報セキュリティ部会が11日の部会で提言をまとめた。管理者の許可なく個人情報を電子的に読み取った場合も、物を盗んだ場合と同様に処罰できるようにする」と報じた。関係資料については（同部会の議事要旨を除き）公開されていない模様である。

有体物の窃盗はともかく、情報の窃盗を安易に刑罰の対象とするのは、構成要件が不明確になるし、罪刑法定主義の観点からも望ましくない。前述のとおり、書店での立ち読みとか電車の中で他人が読んでいる新聞をのぞき込んだだけで「窃盗」となるのは常識に反するだろう。

官僚の側からすると「どこまで取り締まるのサジ加減は我々官僚が決める」という論理になるのだろうが、非常に危険である。官僚の暴走を抑えるためにも、情報窃盗の立法化についてはよく監視しておく必要があろう。

■不法行為法

以上のとおり、情報を漏洩した者に対して刑事責任を問うことは極めて難しい。

そこで、民事訴訟において個人情報を漏洩されてしまった個人が企業・官庁等を訴える場合は、民法709条等の不法行為法に基づき、故意又は過失と発生した損害に対する因果関係を立証して、損害額を請求することになる。

事例としては、宇治市事件（2002年７月最高裁決定）がその先例とされる。

事件が明らかになってから第１審判決（2001年）までの情報は、毎日新聞臺宏士記者の綿密な取材による、記事「個人情報の大量流失事件から2年、京都府宇治市の苦悩」(注1)に詳しい。以下この情報を下に事例分析しよう。

1998年４月ころ、宇治市は、乳幼児検診システムの開発を計画し、外部の民間企業に開発を委託した。市役所内での作業は、就労時間の制約があるので、開発を担当した元大学院生の男性アルバイトは、市の許可を得て、同システムに利用する住民基本台帳と外国人登録名簿の元データ計21万7617件分を持ち帰って作業を行うことになった。

この大学院生は、大阪府の名簿屋に電子メールで購入を打診し、光磁気ディスクに21万人分をコピーして郵送し、５月13日に口座に代金25万8000円が振り込まれたという事件である。事件の起きた98年当時は誰も気づかなかった。問題が判明したのは丸１年後のことである。

翌年1999年５月にインターネットで宇治市の住民票データが販売されていることが判明、市は名簿業者を通じて名簿を回収。６月３日には「完全回収宣言」を市議会総務委員会に報告した。

(注1) 旧リンクはhttp://www.mainichi.co.jp/digital/netfile/archive/200107/17-4.htmlであった。
現在ドメインの変更があったためリンク切れの模様。

また、宇治市は6月10日に宇治署に刑事告発、宇治署はアルバイト男性を「宇治市電子計算機組織に係る個人情報の保護に関する条例」違反で京都地検に書類送検した。

しかし、京都地検は1999年12月、「刑の廃止」を理由に不起訴処分とした。

新条例には、罰則についての旧条例の経過措置に関する明文規定がなかったためだ(一般に、罪刑法定主義により罰則は遡及できない。もっとも、旧条例にも罰則規定はあったのだから単なる立法ミス(経過措置の書き忘れ)ともいえる)。

一方で、宇治市議を含む市民3人が「プライバシーを侵害され、精神的苦痛を受けた」として、同市と大阪市北区の情報処理会社を相手取り、慰謝料など計約200万円の支払いを求めた訴訟を起こした。これ以降、本件は、民事事件として処理されることになる。2001年2月23日、京都地裁の八木良一裁判長は原告側の主張を全面的に認め、被告両者に慰謝料と弁護士費用各1万5000円、計9万円を支払うよう命じた。宇治市は直ちに控訴した。

2001年12月25日大阪高裁(岩井俊裁判長)は、1人につき1万5000円の慰謝料支払いを命じた1審・京都地裁判決を支持し、市の控訴を棄却した。市は最高裁に上告。

そして、2002年7月11日最高裁第一小法廷(藤井正雄裁判長)は、市の上告を棄却する決定を出した。大阪高裁判決が確定した。

■損害賠償額に関する考察など

この事案は、いくつかの点で興味深い。

まず、明らかに情報窃盗して横流しをした者に対して刑事責任を追及できなかったことである。前述のとおり、条例の経過措置立法ミスもあったが、根本的な問題として情報窃盗に対して罪を問うことの難しさがある。

また、一人あたりの損害賠償額が1万5000円とされたことである。これを高いとみるか安いとみるかだが、情報が誰でも閲覧できる基本4情報(氏名、性別、生年月日、住所)くらいであったことからすると、法曹界では妥当な額とされている。この点、前述のYahoo! BB事件では、独自の見解に基づき500円分の金券の配布で済まそうとしたところ、後になって通話記録まで流出したということが報道された事案であり、慰謝の措置として十分といえるのか、批判の強いところでもある。毎日新聞によると被害者の中で一人10万円の慰謝料を求めて大阪地裁に提訴したグループも出てきており
(http://www.mainichi-msn.co.jp/shakai/jiken/news/20040517k0000e040061000c.html)
今後の動向が注目される。

情報漏洩をしてしまった場合、一人あたり1万円以上の損害賠償責任がかかるという通説的な考えをとった場合、1万人分のデータが流出すれば、住基情報程度の簡易な情報でも、「損害賠償額は億のオーダになる」のである。個人情報管理には十分な対策が必要な所以だ。

尾崎孝良氏の紹介

昭和35年生まれ。東京大学理学部数学科卒・英国ケンブリッジ大学Diploma of Computer Science修了という経歴の理系出身の異色弁護士。医事法務のほか、デジタル著作権や情報セキュリティに造詣が深く、各方面で積極的に発言している。最近ではGPL読書会やハッカーのための法律講座などの活動も行っている。情報セキュリティ大学院では、セキュリティの法律実務について教えている。著書に「デジタル著作権」(ソフトバンクパブリッシング)がある。