法的リスクマネジメント講座 第69回

# 機密保持⑤

## ～裁判例特集（その2）～

長谷川俊明法律事務所
弁護士
**長谷川 俊明**

今回は、前回に続き、機密情報などの情報流出を扱った裁判例を紹介します。なお、各事案中で、Xは裁判の原告を、Yは裁判の被告をそれぞれ原則として表します。

### 裁判例5

インターネット接続サービス加入者の個人情報が、顧客データベースの管理業務に従事していた者に不正取得され外部に流出した件に関する大阪地方裁判所平成18年5月19日判決

**事案**

インターネット接続等のサービス（以下、「本件サービス」という。）を共同して提供している被告Y1社及びY2社は、原告Xらが本件サービスの提供に係る契約を両社との間に締結した際、Xらの個人情報を取得した。

Y2社は本件サービスの顧客情報を管理するためリモートメンテナンスサーバーを設置し、同社の業務委託先から派遣されたAに同サーバーの担当者として同サーバーにアクセスするためのユーザー名、パスワードを付与していた。Aは退職後、変更されていなかったユーザー名、パスワードを用いてBと共に顧客情報を不正取得し、Bがこれを Cに渡し、Cがこれを恐喝に利用したが未遂となった。

Y1社とY2社の管理する情報の範囲はそれぞれ異なり、Y1社の分は外部に持ち出されてはいなかった。XらはY1社及びY2社に対し損害賠償を請求した。第一審はY2社の過失だけを認定した。その後原告から控訴がなされ、大阪高裁は、Y1社及びY2社は外形上一体のものとして本件サービスを提供していたと判断し、Y1社の責任も認め、Y2社だけでなくY1社に対してもXら被害者一人につき5,500円の支払いを命じた。最高裁への上告が棄却されたため、大阪高裁の判決が確定した。

**判決要旨**

Y2社は、本件不正取得が行われた当時、電気通信事業者として、当該情報へのアクセスや当該情報の漏えいの防止その他の個人情報の適切な処理のために必要な措置を講ずべき注意義務を負っていたと認められ、リモートアクセスに関しては、顧客データベースサーバーについてリモートアクセスを可能にするに当たって、不正アクセスを防止するための相当な措置を講ずべき注意義務を負っていたと認められる。

本件リモートメンテナンスサーバーに登録されているユーザー名とパスワードについて、Y2社は、①本件アカウントを共有アカウントとしてAが退職した際に、Aが知り得たユーザー名を削除したりそのパスワードを変更したりしなかったこと、②本件リモートメンテナンスサーバーの設置から平成16年1月までの約1年間、登録されているユーザー名について、パスワードの定期的な変更を行わなかったことが認められる。

以上のY2社におけるリモートアクセスの管理体制は、ユーザー名とパスワードによる認証以外に外部からのアクセスを規制する措置がとられていない上、肝心のユーザー及びパスワードの管理が極めて不十分であったといわざるを得ず、Y2社は、多数の顧客に関する個人情報を保管する電気通信事業者として、不正アクセスを防止するための前記注意義務に違反したものと認められる。

【解説】

この事件では、サーバーへのアクセス管理、アカウント付与についての委託元の管理体制が問われました。委託元は、第三者の故意・過失による情報流出事故の事後対応、委託業務が終了した後の処理を含めたクライシス・マネジメントの備えについても万全を期す必要があります。

### 裁判例6

会社が顧客情報を漏洩させた元社員に対し損害賠償を請求した件に関する長崎地方裁判所佐世保支部平成20年5月15日判決

**事案**

平成10年ごろ、原告X社の元従業員である被告YとAの共謀により、X社の顧客情報約51万人分（顧客の住所、氏名、生年月日、性別及び電話番号等）（以下「本件顧客情報」という。）が流出した。

平成16年、漏洩が発覚し、X社は営業を自粛した。X社は賠償を求めて民事調停を申し立て、調停で漏洩への関与を認めたAとは調停が成立した。Yは関与を否定した。X社が判例を基に漏洩の損害を一人あたり5千円程度で約25億7千万円と試算し、Yの弁済能力を考えて漏洩につき約6,300万円を請求する訴訟を提起した。その判決で、長崎地裁はX社の請求通りの金額の支払いを命じた。

**判決要旨**

平成16年3月に本件顧客情報漏洩が発覚し、X社が49日間の営業自粛に踏み切ったこと、その後、X社は、同年11月までは、営業自粛を続けたこと、その間、X社は、信用回復のための種々の対処を余儀なくされたことが認められる。さらに、本件顧客情報が当該顧客を特定し、当該顧客へのアクセスを容易にするような基本的な情報を内容とするものであったこと、このような個人情報が大量に流出し、そのことが新聞・テレビ等において大きく報道されたことにより、顧客情報を大量に保有・管理するX社の信用は大きく失墜したといえることを考慮すれば、X社の上記営業自粛は、本件漏洩を前提とするX社の対応として、必要かつ相当な対応であったといえる。

【解説】

会社の保有する情報を漏洩させた者に対して会社のとりうる法的手段としては、被害者に賠償を支払ってから求償するほかに直接の損害賠償請求があります。本裁判例は、X社の対応を「必要かつ相当」と認定しており、会社側の請求をほぼ認めた裁判例として注目されています。

### 裁判例7

元社員が会社の顧客情報を利用し顧客に営業上の信用を害する虚偽の事実を告知したとして、2社が損害賠償を求めた件に関する知的財産高等裁判所平成24年7月4日判決

**事案**

投資用マンションの販売を業とするX1社の営業社員であったY1とY2は、X1社とその子会社でX1社が販売した不動産の賃貸管理等を業とするX2社の顧客情報を取得して退職した。Y1は、投資用マンションの賃貸管理等を業とし、X2社と競業関係にあるY3社を設立して、Y2を雇用した。

Y1とY2は上記顧客情報を使用してX1社とX2社の顧客に連絡し、X1社とX2社の営業上の信用を害する虚偽の事実を告知するとともに、不正な利益を得る目的または顧客情報を保有するX2社に損害を加える目的で、賃貸管理の委託先をX2社からY3社に乗換するよう勧誘して賃貸管理委託契約を締結した。X1社とX2社は営業秘密の不正取得・使用等に基づく損害賠償等を求めて訴えを提起し、第一審がX1社らの請求の一部を認めたため、Y1とY2及びY3社が控訴した。控訴審は、Y1とY2及びY3社の控訴とX1社の附帯控訴*1を棄却し、X2社の附帯控訴について第一審判決の一部を変更して、請求を一部認めた。

*1 附帯控訴
控訴があった場合に控訴された側の者が行う、第一審判決のうち自分に不利な部分の変更を求める申立て。

**判決要旨**

本件顧客情報はX1社の営業部を統括する営業本部により、顧客ファイルや顧客管理システムに保管された電子データとして一元管理されており、顧客ファイルや顧客管理システムはいずれも入室が制限された施錠付きの部屋に保管されている上、その利用も、前者は営業本部の従業員と所定の申請手続を経た営業部所属の従業員に限定されている。

X1社とX2社は、各部内に常備された本件就業規則で秘密保持義務を規定するとともに退職時に秘密保持に関する誓約書を提出させたり、各種の情報セキュリティを実施してISMS認証*2やISO／IEC27001認証を取得し、毎年行われる審査に合格したり、従業員に対する「ISO27001ハンドブック」の配布やこれに基づく研修・試験といった周知・教育のための措置を実施したりしていたのであるから、X1社とX2社は従業員に対して、本件顧客情報が営業秘密であると容易に認識しうるようにしていたものといえる。

以上を総合すれば、X1社とX2社は、本件顧客情報に接し得る者を制限し、本件顧客情報が秘密であると認識し得るようにしていたといえるから、本件顧客情報は、2社の秘密として管理されていたということができる。

*2 ISMS認証とISO／IEC27001認証
ISMS認証は情報セキュリティマネジメントシステムの国内規格。ISO／IEC27001認証は上記システムの国際規格。

【解説】

本裁判例は、アクセスの制限、アクセス可能な者にその情報が秘密であると認識し得るようにしていたことを根拠に、不正競争防止法の「営業秘密」の要件である秘密管理性を肯定しています。経済産業省の営業秘密管理指針における秘密管理に関する記述とともに参考にすべきでしょう。

### おわりに

いま、事業遂行上の“生命線”ともいえる「営業秘密」が企業から盗まれたりして外部に流出するケースが増えています。

とくに中小の製造業にとって、「営業秘密」の適切な管理は会社の存続を左右する重要課題になったといえそうです。

新日鉄住金が、同社の高機能鋼板の製造技術を不正取得したとして韓国鉄鋼大手ポスコなどを相手取り損害賠償などを求めていた訴訟で、2015年9月30日、和解が成立しました。

和解内容は、ポスコが同日、新日鉄住金に300億円を支払い、両社は日本、韓国、米国で起こした訴訟を取り下げるというものでした。ただ、新日鉄住金の、“盗用”に関与した元社員に対する訴訟は継続しています。

2015年7月には、不正競争防止法が改正され「営業秘密」の不正取得は罰金額の引き上げなどにより罰則が強化されました。法律による情報流出抑止力は増したのですが、企業の管理体制が甘ければ罰則を科すことはできません。

情報管理体制をしっかり構築した上で、“不正”には法廷闘争も辞さずとの毅然とした態度が求められます。