《第3回》

情報漏えい事案に関する裁判例にみる企業の責任(2)

法律事務所クロス
弁護士 山岡裕明

前号のⅡ1(2)に引き続き，情報漏えい事案に関する裁判例を紛争当事者類型別に紹介する。

(3) 個人情報取得者―システム開発受託者間

この紛争類型は，紛争当事者間に情報システムの開発・保守に関する業務委託契約があることから，基本的に訴訟物は債務不履行責任に基づく損害賠償請求権となる。

・unico個人情報漏えい事件[1]

① 事案の特徴

漏えい原因	システム開発受託者（被告）が製作したアプリケーションに脆弱性があったことからSQLインジェクション[2]というサイバー攻撃により個人情報取得者（原告）のサーバから個人情報が漏えいした。
請求内容	個人情報取得者である発注者（原告）のシステム開発受託（被告）に対する債務不履行に基づく損害賠償請求。

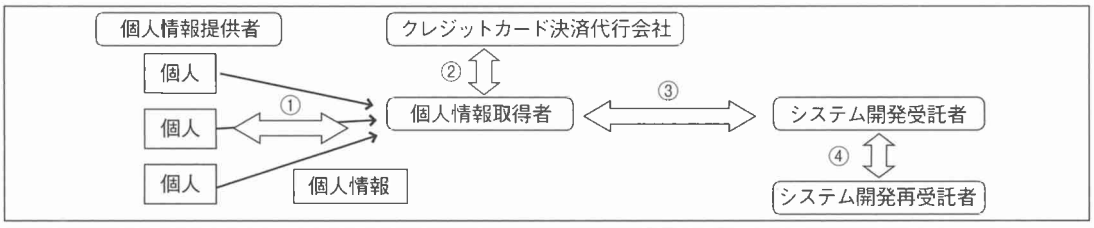
② 判旨の特徴

a．個人情報の機密性を保持する義務

システム開発受託者（被告）は，個人情報取得者（原告）とのシステム発注契約の時点において「その当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供することが黙示的に合意されていた」として，「当該個人情報の漏洩を防ぐために必要なセキュリティ対策を施したプログラムを提供すべき債務を負っていた」とした。

そして，当該債務の具体的な範囲について，その当時，経済産業省および独立行政法人情報処理推進機構（以下「IPA」という）がSQLインジェクション攻撃によってデータベース内の大量の個人データが流出する事案が相次いで発生しているとの注意喚起を文書において行い，また，その対策としてSQL文の組み立てにバインド機構[3]を使用し，またはSQL文を構成するすべての変数に対しエス

【図表】情報漏えい事案の紛争当事者



[1] 東京地判平26.1.23判時2221号71頁。

[2] SQLインジェクションとは，ウェブアプリケーションの入力画面にプログラム作成者の予想していない文字列を入力することにより，不正なSQL（Structured Query Language）文を実行させることである。入力された不正なSQL文がそのまま実行される結果，本来ウェブサービスが想定していない操作が行われ，非公開の情報が取り出されたり，ウイルスをダウンロードさせる仕掛けを埋め込まれる。

[3] バインド機構とは，あらかじめプログラム作成者が想定したSQL文だけを実行できるようにするメカニズムをいう。

ケープ処理[4]を行うことをあげていたことから，システム開発受託者（被告）は，「顧客の個人情報が漏洩することを防止するために，SQLインジェクション対策として，バインド機構の使用又はエスケープ処理を施したプログラムを提供すべき債務を負っていた」と認定した。

すなわち，経済産業省およびIPAの文書という公的規範の存在およびウェブアプリケーションという情報システムに内在するリスクをふまえて義務が導かれている。

b．過　失

システム開発受託者（被告）が「プログラムに関する専門的知見」を有することからその「注意義務の程度は比較的高度なもの」であることを前提に，「SQLインジェクション対策がされていなければ，……個人情報が流出する事態が生じ得ることは被告において予見が可能であり」，かつ，経済産業省およびIPAがSQLインジェクションの対応策について注意喚起していたことから，当該予見は「容易であ」り，さらに，当該対応策を行うことに「多大な労力や費用がかかることをうかがわせる証拠』はないので，「本件流出という結果を回避することは容易」であったとして，重過失が認定された。

c．コメント

一般的に，システム開発の中でセキュリティ対策を強化すると開発の工数が増すので，開発費は増加する。そこで，費用対効果の観点から，セキュリティ対策については契約上必要最低限に留めることが少なくない。本件でも「SQLインジェクション」という攻撃についての具体的なセキュリティ対策は明記されていなかった。

本件では，「SQLインジェクション」という攻撃手法およびその対策が周知されていたために「黙示の合意」に基づきSQLインジェクション対策の義務が導かれているが，本来的には契約に具体的なセキュリティ対策を明記しない限り，同対策についての義務が否定されてもおかしくない。

システム開発を発注する企業としては，少なくとも典型的なサイバー攻撃に対するセキュリティ対策についての説明を受け，適切に契約に盛り込む必要がある。

(4)　システム開発受託者―システム開発再受託者間

この紛争類型は，紛争当事者間においてシステム契約の開発・保守に関する業務委託契約が存在するという点において，(3)の紛争類型と類似する。

・愛南町個人情報流出事件[5]

①　事案の特徴

漏えい原因	システム開発再受託者（被告）の従業員が個人情報を貸与パソコンに保存のうえ，当該パソコンを自宅に持ち帰り，自宅にある夫のパソコンに当該個人情報を保存したところ，ウイルスの感染が原因で当該情報が流出した。
請求内容	システム開発受託者（原告）のシステム開発再受託者（被告）に対する，主位的に使用者責任，予備的に債務不履行に基づく損害賠償請求。

[4] エスケープ処理とは，SQL文において特別な機能を持つ記号文字を無効化，すなわち普通の文字として解釈されるようにする処理である。たとえば，エスケープ処理をしないと「'」は単なるシングルクオーテーションとしての記号ではなく，文字列定数の終端という特別の機能を持つものとして解釈されてしまうところ，同処理をすることにより，単なるシングルクオーテーションを表す記号として解釈させることが可能となる。

[5] 山口地判平21.6.4裁判所HP参照（平成19年（ワ）第331号）。

② 判旨の特徴

a．被用者の選任・監督についての過失について

個人情報の漏えいについて従業員に不法行為責任が成立することを前提に，使用者責任の有無が争点となった。システム開発再受託者（被告）は，「当時ウィニーによる情報の漏洩事故の発生は余り知られておらず，本件従業員が貸与パソコンに保存していた個人情報を夫のパソコンに移すとか，本件従業員の夫が同パソコンにウィニーをインストールすることまでは予見不可能であり，それを前提とする指導・監督をすることまでは求められていない」旨を主張したのに対して，本判決は，「従業員が，貸与パソコンのデータを夫のパソコンに取り入れた当時には，既にウィニーによる情報漏洩事故は多発しており，そのことは少なくとも個人情報を取り扱う事業者の周知するところとなっていたと認められるから，ウィニーによる個人情報の漏洩も予見できたというべきである」として使用者責任を肯定した。

b．コメント

北海道警察捜査情報漏えい事件（**前号Ⅱ1(1)(イ)**）と同様，ウイルスを原因とする個人情報の漏えいにつき，過失，特に予見可能性の有無が問題となった事案である。

ウイルスに限らずサイバー攻撃全般において，企業としてどの時点で対応策をとっていないとその過失責任が肯定されるか，という点において示唆に富む事案である。

すなわち，同じくウイルスを原因とする情報漏えいについての予見可能性を論じた北海道警察捜査情報漏えい事件の第二審判決では，個別具体的に検討のうえ予見可能性を否定したのに対して，本判決は，単に「ウィニーによる情報の漏洩事故が多発していることは周知の事実であった」および「本件従業員が，貸与パソコンのデータを夫のパソコンに取り入れた当時には，既にウィニーによる情報漏洩事故は多発しており，そのことは少なくとも個人情報を取り扱う事業者の周知するところとなっていた」として，「ウィニー」という名称のウイルスを原因とした情報漏えい事件が周知の事実であったことを理由に使用者責任を肯定している。

サイバー攻撃における過失の認定にあたっては，当該攻撃の周知性が1つの重要な指標となっている。

したがって，サイバーセキュリティ体制の整備にあたり，周知性のあるサイバー攻撃への対応から優先的に進めることが重要となる。

2 論点別の検討

以下，これまで紛争当事者ごとに紹介した裁判例において問題となった論点を個別に紹介する。

主要な論点としては，情報漏えいを防止すべき義務，過失，使用者責任における指揮監督関係の有無である。

(1) 情報漏えい防止義務

情報漏えい事案においては，個々の裁判例ごとに呼称の違いはあれど，情報の機密性を保持すべき義務（以下便宜上「情報漏えい防止義務」という）の有無および内容が問題となる。

情報漏えい防止義務は一律に導かれるわけではなく，以下で検討するとおり，公的規範，主体（事業）の属性，採用している情報システムに内在するリスクおよび情報の内容といった要素が考慮される傾向にある。

(ア) 公的規範

情報漏えい防止義務を認定するにあたり，多くの場合公的規範が参照される。

Yahoo！BB顧客情報漏えい事件（**前号Ⅱ**

1(1)(ウ)) は個人情報保護法，電気通信事業における個人情報保護に関するガイドライン，JIS規格およびコンピュータ不正アクセス対策基準を，TBC事件（**前号Ⅱ1(1)(エ)**）はOECDおよび民間部門における電子計算機処理に係る個人情報保護に関するガイドラインを，愛南町個人情報流出事件は個人情報保護法を，unico個人情報漏えい事件は経済産業省による「個人情報保護法に基づく個人データの安全管理措置の徹底に係る注意喚起」と題する文書およびIPAによる「大企業・中堅企業の情報システムのセキュリティ対策～脅威と対策」と題する文書を参照して，情報漏えい防止義務を論じた。

個人情報保護法は公法上の業規制にすぎず，直接的には民事上の注意義務を構成するものでない。また，その他のガイドラインおよび文書も少なからず公的性質を有するとはいえ，自主規制であったり民間に対する注意喚起の呼びかけにすぎず，民事上の注意義務を構成するものでない[6]。TBC事件の第一審判決も「これらのガイドラインは，直ちに不法行為における注意義務を構成するものではない」とあえて指摘するところである。

しかしながら，これらの公法，ガイドラインおよび公的性質を有する文書に含まれる公的規範は，いずれも個人情報保護の重要性およびその時点における個人情報を保護するための技術水準を反映するものであり，私法上の注意義務の有無および内容を導くうえで1つの重要な指針となっている。上記のTBC事件の第一審判決も「これらのガイドラインは，直ちに不法行為における注意義務を構成するものではない」としつつも，続いて「そこで要請されている個人情報保護の必要性にかんがみると，……個人情報を取り扱う企業に対しては，……個人情報保護のために安全対策を講ずる法的義務が課せられていた」と指摘する。

(イ) 主体（事業）の属性

情報漏えいの原因に関与した主体（事業）の属性も，情報漏えい防止義務の内容を確定するにあたり重要な要素となっている。

北海道警察捜査情報漏えい事件の第一審判決は，警察官としての立場を重視して，「警察官として捜査上の情報を厳重に管理して外部流出を防止すべき注意義務を負っている」とした。

Yahoo！BB顧客情報漏えい事件の第一審判決は，当該個人情報取得者が電気通信事業法上の電気通信事業者に該当することを認定のうえ，「顧客の個人情報を保有，管理する電気通信事業者として，当該情報への不正な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管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」とした。

TBC事件は，システム開発受託者の注意義務を論じるにあたり「インターネット及びイントラネット構築，WWWホスティングサービス，サーバー構築及びウェブサイトのコンテンツ作成などを事業の目的とする企業」たる同システム開発受託者の「その提供する業務に関する技術的水準」を詳細に検討のうえ，具体的な義務を認定している。

(ウ) 情報システムに内在するリスク

以下で取り上げるリモートアクセスおよびウェブアプリケーションは，いずれも業務活動において重要な情報システムである反面，それぞれ固有のリスクが内在する。こうした情報システムに内在する固有のリスクが情報漏えい防止義務を確定するにあたり重要な要素となる。

---

6 宇賀克也『個人情報保護の理論と実務』（有斐閣，2009）61頁。

① リモートアクセスに内在するリスク

リモートアクセスについては，その仕組み上，リモートサーバを通じた社内ネットワークへの不正侵入，外部端末に保存した情報の漏えい，リモートアクセス通信の盗聴といったセキュリティ上の固有のリスクが指摘されている。

こうしたリスクをふまえ，Yahoo！BB顧客情報漏えい事件の第１審判決は，「あるサーバーに対してリモートアクセスを可能にすることは，それ自体，当該サーバーに対する外部からの不正アクセスの危険を高めるものであ」り，「リモートアクセスを可能にするに当たっては，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いうべきである」とした。

② ウェブアプリケーションに内在するリスク

ウェブアプリケーションには，その開発過程において脆弱性が生じやすく，脆弱性があるとそれを利用した攻撃がなされ，個人情報の漏えいを招く。

また，SQLインジェクション，クロスサイトスクリプティング等といった代表的なサイバー攻撃の手法が確立されている。

unico個人情報漏えい事件は，システム開発受託者が製作したアプリケーションに脆弱性があったことからSQL インジェクションにより個人情報取得者のサーバから個人情報が漏えいした事案であるが，当該システム開発受託者には「当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供することが黙示的に合意されていたと認められる」とした。

(エ) 情報の内容

漏えいした個人情報の内容も，情報漏えい防止義務の有無および内容を導くにあたり重要な要素となりうる。

住民基本台帳のデータが漏えいした事案である宇治市住民基本台帳データ漏えい事件（**前号Ⅱ１(1)(ア)**）の第二審判決は，取得対象となる情報が「プライバシーに属する情報」であるという情報の性質をふまえ，個人情報取得者は，「その秘密の保持には万全を尽くすべき義務を負うものというべきである」とした。

通常の個人情報に加え，アンケートを通じて回答したエステティックサービスの「コース内容」や個別の「質問に対する回答」が漏えいした事案であるTBC事件の第二審判決は，「一層慎重な配慮のもとに顧客の個人情報を厳密な管理下で扱わなければならないと解すべきである」と判示し，情報の内容によっては，より一層厳格に管理する義務の存在を示している。

本年５月30日に施行された改正個人情報保護法により，新たに「要配慮個人情報」が定義された関係で，要配慮個人情報またはそれに準ずる情報については，通常の個人情報と比べて今後はより一層厳格に管理する義務が認められる可能性がある。

また，顧客のクレジットカード情報が漏えいした事案であるクーポン購入サイトクレジットカード情報漏えい事件は，「本件サイトは，クレジットカードの情報という機密性の高い情報を扱うサイトであるから，それに応じた高度のセキュリティ対策が必要というべきであり」として，機密性の高い情報とそうでない情報との間で，セキュリティ対策の義務の程度が異なることを示している。

＊ 次号はⅡ２(2)以降を掲載します。

山岡裕明（やまおか ひろあき）
法律事務所クロス弁護士。2010年弁護士登録。情報セキュリティスペシャリスト。情報法を専門とし，知財紛争，システム紛争，ドメイン紛争，企業の情報管理対応を中心に扱う。