《第2回》

情報漏えい事案に関する裁判例にみる企業の責任(1)

法律事務所クロス
弁護士　山岡裕明

Ⅰ　はじめに

本号からは，裁判例を参考にサイバーセキュリティに関する企業の責任を紹介する。

前号において，サイバーセキュリティの一部として情報セキュリティがあり，情報セキュリティには三要素があることを紹介した。この三要素の１つである機密性に係る問題として情報漏えい事案があり，特にこの種の事案において，企業の法的責任に関する裁判例の集積が見られる。

他方で，それ以外の分野（サイバーセキュリティのうち情報セキュリティ以外の分野，および情報セキュリティの三要素のなかでも完全性および可用性についての分野）に関する裁判例は今のところ見当たらない。

もっとも，個人情報の漏えい事案であれ，それ以外の分野に関する事案であれ，企業の責任が問われる場合の法律構成および争点は大きく異ならないはずである。ウイルスによるサイバー攻撃を想定すると，ウイルス感染を原因とした個人情報の漏えいを理由に個人が企業に対して損害賠償請求をする場合，当該企業の情報の機密性を保持する義務および過失の有無が主要な争点となる。他方，本年５月の世界同時サイバー攻撃の際，ランサムウエアというウイルスによりパソコンやサーバー内のデータ（情報）が暗号化されて使えなくなった結果，英国の病院では手術が中止されたと報道されたが，仮に手術を受ける予定であった患者がこの中止により病状が悪化したとして同病院に対して損害賠償請求をする場合，当該病院の情報の可用性を保持する義務および過失の有無が問題となるはずである。そして，機密性を保持する義務であれ，可用性を保持する義務であれ，その具体的な義務の内容は，事実上かなり重複することになる。ウイルスの感染自体を事前に防ぐことが義務[1]の重要な内容となり，情報が漏えいするかデータが暗号化されるかは感染したウイルスの機能の違いにすぎないからである。

そうだとすれば，個人情報の漏えい事案における企業の法的責任に関する裁判例の検討は，広くサイバーセキュリティ全般における企業の法的責任についても応用が効くものと考える。

以下，個人情報の漏えい事案に関する主要な裁判例を便宜上紛争当事者ごとに分けて紹介のうえ，そこで抽出した論点を，改めて論点別に整理する予定である。

Ⅱ　裁判例の検討

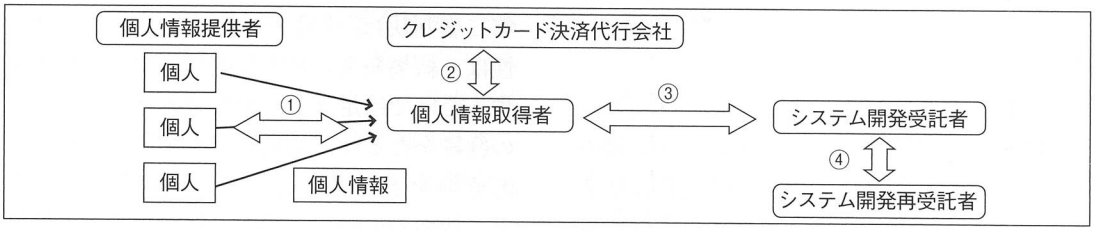
1　紛争当事者別の検討

情報漏えい事案の紛争当事者は，大きく分けて次の５者が関係する。

まず，漏えいした個人情報に係る個人（以

[1] 全社的にウイルス対策ソフトを導入する，外部からのメールに添付されたファイルを不用意に開封しないよう徹底する，OSやソフトウェアを逐次アップデートさせる等が考えられる。

【図表】情報漏えい事案の紛争当事者



下「個人情報提供者」という）および個人情報を取得した企業（以下「個人情報取得者」という）である。

また，電子データ化された個人情報を管理するための情報システムの開発・保守業務を個人情報取得者から受託する者（以下「システム開発受託者」という），およびシステム開発受託者から当該業務をさらに受託する者（以下「システム開発再受託者」という）も紛争当事者となる。

さらに，個人情報取得者がその決済においてクレジットカード決済代行会社を利用していることも少なくない。

裁判例上，情報漏えい事案の紛争当事者は，【図表】のとおり４つの類型に分けることができる。そして，訴訟物もおおむねこの類型ごとに整理することができ，①は不法行為に基づく損害賠償請求権，②，③および④は債務不履行に基づく損害賠償請求権となる。

(1) 個人情報提供者―個人情報取得者間

この紛争類型は，情報漏えい事案において最も多い類型である。

主要な争点としては，不法行為責任（民法709条）の場合には個人情報取得者が負う個人情報の機密性を保持する義務の内容および予見可能性を中心とした過失の有無，使用者責任（同法715条）の場合には指揮監督関係の有無があげられる。また，以下に検討する裁判例には，個人情報取得者が地方自治体の場合を含み，その場合には訴訟物が国家賠償法１条１項に基づく損害賠償請求権となるが，その要件・効果は使用者責任とほぼ共通しているため，ここであわせて紹介する。

(ア) 宇治市住民基本台帳データ漏えい事件[2]

① 事案の特徴

漏えい原因	システム開発再受託者の従業員Xが，住民基本台帳のデータを自分のコンピュータにコピーして持ち出した。
請求内容	個人情報提供者である住民（原告）の個人情報取得者である宇治市（被告）に対する民法715条または国家賠償法１条１項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

第一審判決は，指揮監督関係を論じる前提としてではあるが，住民基本台帳の「データが，……個々の住民のプライバシーに属する情報である以上，被告は，その秘密の保持には万全を尽くすべき義務を負う」として，「プライバシーに属する情報」であるという取得情報の性質をふまえ，個人情報取得者が「秘密の保持には万全を尽くすべき義務」を負うとした。

b. 指揮監督関係

第一審および第二審を通して，個人情報取得者は，Xが宇治市の職員でないため，指揮監督する権限はなかったと主張した。第二審判決は，この点につき「実質的な指揮・監督関係の有無によって決するのが相当」としたうえで，Xが個人情報取得者の担当者との打ち合わせに参加していたこと（協議の存在），

[2] 京都地判平13.2.23判例地方自治265号17頁および大阪高判平13.12.25判例地方自治265頁11頁。

およびXが個人情報取得者の庁舎内で作業を行っていたこと（作業場所）を考慮のうえ，実質的な指揮監督関係を肯定した。

c. コメント

個人情報取得者の立場からすると，直接の契約関係にないシステム開発再受託者の従業員に起因する情報漏えいまで使用者責任が肯定されうる点には注意が必要である。

(イ) 北海道警察捜査情報漏えい事件[3]

① 事案の特徴

漏えい原因	巡査が被疑者の個人情報を含む捜査情報を私用パソコンに保存し，自宅に持ち帰ったうえ，インターネットに接続したところ，同パソコンがコンピュータウイルスに感染していたことが原因で同情報を外部に流出させた。
請求内容	個人情報提供者である被疑者（原告）の個人情報取得者である北海道（被告）に対する国家賠償法１条１項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

第一審判決は，「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」があるとして，「警察官」という管理主体の属性および「捜査上の情報」という情報の性質をふまえ，情報を「厳重に管理して外部流出を防止すべき注意義務」を認定した。

b. 過失（主に予見可能性）

過失の内容は，一般的に損害発生に対する予見可能性および結果回避義務が考慮される。ウイルスに限らず，新しい手法によるサイバー攻撃がなされた場合，この予見可能性が最も大きな争点となりうる。

本件は，この予見可能性の点で第一審判決と第二審判決との間で判断が分かれた示唆に富む事案である。

すなわち，第一審判決が抽象的かつ比較的緩やかに予見可能性を認定したのに対して，第二審判決は，「過失の前提となる予見可能性は，結果発生に対する抽象的な危険を予見するだけでは足りず，加害者の行為から一定の経緯をたどって結果が発生するという具体的危険を予見することが必要」としたうえで，個別の事情を具体的に検討のうえ予見可能性を否定した。

c. コメント

サイバーセキュリティの確保にあたっては，経営判断として費用対効果を考慮せざるをえない。第二審判決は，ウイルスによる損害発生についての具体的危険が予見不可能な場合にその過失を否定している点で，日々登場するあらゆる脅威に対して万全のサイバーセキュリティの確保を要求するものではないということを示すものである。

ただし，新たな手法によるサイバー攻撃であっても，大々的に報道されているサイバー攻撃については，損害発生についての予見可能性が認められうるので早急に対策を講じる必要がある。

(ウ) Yahoo！BB顧客情報漏えい事件[4]

① 事案の特徴

漏えい原因	業務委託先から派遣されたXが，退職後，その在職中に知ったアカウント情報（ユーザー名およびパスワード）を用いて，外部のパソコンから個人情報取得者のサーバにリモートアクセスして，顧客情報を不正に取得した。
請求内容	個人情報提供者である顧客（原告）の個人情報取得者（被告）に対する不法行為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

第一審判決および第二審判決はともに，個人情報取得者が電気通信事業法の電気通信事業者および個人情報保護法上の個人情報取扱

[3] 札幌地判平17.4.28判例地方自治268号28頁および札幌高判平17.11.11（LEX/DBインターネット28102361）。

[4] 大阪地判平18.5.19判時1948号122頁および大阪高判平19.6.21判例集未登載。

事業者であることを前提に，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５条４項および個人情報保護法20条の規定を考慮して，「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。

さらに，第一審判決はリモートアクセス固有のリスクをふまえ，「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」とした。

すなわち，被告の主体の属性，個人情報保護法およびそのガイドラインという公的規範の存在ならびにリモートアクセスという情報システムに内在するリスクをふまえて，注意義務が導かれた。

b. 過　失

第一審判決および第二審判決はともに，個人情報取得者（被告）の過失を肯定している。第一審判決は，予見可能性および結果回避可能性に分け，前者につき個人情報取得者がXに行わせていた業務の内容および与えていた権限の内容等を考慮のうえ，「Xが業務を終えた後に，業務中に知り得たパスワード等の情報を用い……ることによる不正アクセスについては，予見可能であった」とし，続いて後者につき，「アカウントを含むユーザー名・パスワードの適切な管理等，不正アクセスを防止するための相当な措置を採っていれば防ぎ得たといえるから，結果回避可能性も認められる」とした。第二審判決は，結果回避可能性について，さらに具体的に「Xが退職した後に，本件アカウントを含め，Xが知り得たユーザー名を削除したり，パスワードを変更するなどの措置を採るべきであった」として代替手段の存在を理由に結果回避義務違反を肯定した。

c. コメント

アカウント情報の管理を含むアクセス権限の適切な管理は，サイバーセキュリテイにおける基本事項である[5]。管理画面からアカウント情報を入力してデータにアクセスすることができれば，高度な技術力がなくともサイバー攻撃は可能となるからである。

そうすると，企業としては，アカウント情報が簡単に推測または利用されない体制整備がまずもって重要であり，これを怠った場合には，比較的緩やかに過失が肯定される点に注意が必要である。

(エ) TBC事件[6]

① 事案の特徴

漏えい原因	サーバ移転作業の際，システム開発受託者が個人情報を格納した電子ファイルをインターネット上誰でも閲覧できる状態に誤って置いた結果，第三者が同ファイルにアクセスしてインターネット上に流出させた。
請求内容	個人情報提供者である顧客（原告）の個人情報取得者（被告）に対する使用者責任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

第一審判決は，OECDおよび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，その事業内容等に応じて，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」とした。

b. 指揮監督関係

ウェブサイトの制作・保守についての専門的技術的な知識がないためシステム開発受託者に対し実質的に指揮監督する地位になかっ

[5] 情報システム安全対策指針（平成９年国家公安委員会告示第９号）はネットワークおよびホストへのアクセスについて「ログインに際し，識別及び認証を行うこと」と規定する。

[6] 東京地判平19.2.8判タ1262号270頁および東京高判平19.8.28判タ1264号299頁。

たという被告の主張について，第一審判決は，「本件ホームページ制作保守契約においては，本件ウェブサイトのコンテンツの内容等は被告が決定し」，システム開発受託者は，「その決定された内容を実現するために専門的技術的知識を提供するにすぎ」ないとして，指揮監督関係を肯定した。

c. コメント

一般的に，個人情報を含む電子データを管理する情報システムの開発および保守に関する業務について，それらの全部または一部を外部に委託することも珍しくない。

たしかに，情報システムの専門的技術的知識が十分ではないためシステム開発受託者の業務を詳細に把握することは容易ではないとしても，専門的技術的知識の不足をもって，指揮監督を免れるわけではないことに注意が必要である。

(2) クレジットカード決済代行会社―個人情報取得者間

この紛争類型は，紛争当事者間に契約関係があることから契約責任が問題となる。

(オ) クーポン購入サイトクレジットカード情報漏えい事件[7]

① 事案の特徴

漏えい原因	漏えい原因の詳細について明らかになっていないが，少なくとも「本件サイトに何らかの不正なアクセス等が行われることによって被告の顧客のクレジットカード情報が漏えいしたことが推認」されている。
請求内容	クレジットカード決済代行会社（原告）の個人情報取得者（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

クレジットカード決済代行会社（原告）の約款に規定された個人情報取得者（被告）の「会員のカード情報等を第三者に閲覧されないように本件サイトを適切に管理する義務」を前提に，個人情報取得者（被告）がレンタルサーバを利用していたことをもって，同義務が履行されていたか否かが争われた。

この点につき「いかなる程度のセキュリティ対策を取るかについては，当該セキュリティ対策を取るために必要となる費用や当該サイトで取り扱っている情報の内容とそれに応じた秘密保護の必要性等の程度を勘案して，適切な程度のセキュリティ対策を取ることが必要というべきである」ところ，「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」るが，被告が利用した「レンタルサーバ契約は，一般的なレンタルサーバに係るものにすぎ」ず，当該契約に「標準で付されているセキュリティ対策が，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のに適した程度のもの……と推認することはできない」として義務違反が認定された。

b. コメント

サーバのレンタルを含むいわゆるホスティングサービスには，セキュリティ対策も含まれていることがほとんどであるが，その内容は，利用料金によって異なる。

したがって，企業が外部のホスティングサービスを利用するにあたって，特にクレジットカード情報のような機密性の高い情報を扱う場合には，相応のセキュリティ対策が含まれたサービスを利用することが必要となる。

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。

[7] 東京地判平25.3.19判例集未登載。