《最終回》

情報漏えい事案に関する裁判例にみる企業の責任(3)

法律事務所クロス
弁護士　山岡裕明

前号のⅡ2(1)に引き続き，情報漏えい事案に関する裁判例にみる主要な論点を個別に紹介する。

(2)　過　失

過失の概念を整理すると，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の2つの要素が考慮される[1]。

サイバーセキュリティの分野は，そもそも極めて専門技術性が高い分野であり，かつ，新たな手法のサイバー攻撃が次々と登場する。こうした特殊性から，サイバー攻撃に起因する損害発生に対する予見および結果回避は必ずしも容易ではない。そこで，過失の有無が主要な争点となる。

(ア)　予見可能性

①　具体性の程度

捜査情報を保存した私用パソコンがウイルスに感染していたため捜査情報が漏えいした事案である北海道警察捜査情報漏えい事件（**11月号Ⅱ1(1)(イ)**）において，第一審判決は「パソコンをインターネットに接続した場合にパソコン内の情報が本人の知らないうちに漏えいする危険があることは当然認識し」，かつ，「私有パソコン内に残存する公務に関する情報が私的な使用の際に外部に流出する危険は十分に予想される」として，問題となったウイルスの特性を個別具体的に論じることなく，抽象的にウイルス感染による情報漏えいについての予見可能性を論じた。サイバーセキュリティに対する脅威は，多種多様である。ウイルス1つとっても，感染原因および機能が異なり，最新のウイルス対策ソフトを導入していても対応できない場合がある。こうしたサイバーセキュリティに対する脅威を過度に抽象化しては過失が緩やかに認定されることになりかねない。この点につき，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である」とし，具体的危険を予見することを要求した。

②　考慮要素

具体的危険についての予見可能性を判断するにあたり，サイバーセキュリティに対する脅威についての周知性が重要な指標となる。すなわち，当該脅威についての周知性がなければ，サイバーセキュリティに関する専門的知識がない限り，当該脅威の具体的危険を予見することは困難であるし，他方で，脅威に対する周知性が認められるのであれば，情報

[1] 我妻榮＝有泉亨＝清水誠＝田山輝明『我妻・有泉コンメンタール民法―総則・物権・債権〈第4版〉』（日本評論社，2016）1334頁は，「過失の概念を分析すると，第1に，加害行為を行った者が，損害発生の危険を予見したこと，ないし予見すべきであったのに（予見義務）予見しなかったこと（予見ないし予見可能性）と，第2に，損害発生を予見したにもかかわらず，その結果を回避するべき義務（結果回避義務）に違反して，結果を回避する適切な措置を講じなかったという，二つの要素が認められると考えるのが，一般的になっている」とする。

セキュリティの専門的知識がなくとも，当該脅威の具体的危険を予見することは困難ではない。持ち帰った個人情報を自宅にある夫のパソコンに保存したところ，当該パソコンがウイルス「ウィニー」に感染していたため個人情報が漏えいした事案である愛南町個人情報流出事件判決（**12月号Ⅱ 1(4)**）は「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」こと，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」（下線は筆者による。以下同じ）とし，ウイルスという脅威についての予見可能性の根拠として，その周知性に言及した。

周知性を判断するにあたって，裁判例上，以下の諸要素が参考になる。

a．脅威の新規性

北海道警察捜査情報漏えい事件の第二審判決は「アンティニーGが，それまでのウイルスと異なる，パソコン内の情報が外部に開示・流出するという新たな特質を有する」と判示した。脅威に新規性があれば，一般に当該脅威についての周知性は低いといえ，その予見は困難といえる。

ただし，脅威の新規性は，新規か否かの２択というよりはどの点がどの程度新規性を有するかという問題であることに留意を要する。たとえば，日本年金機構における個人情報漏えい事件で話題となった標的型攻撃メールにおいては，メールの添付ファイルを開封したりメール本文に記載されたリンク先にアクセスしたりすることでウイルスに感染するものであるが，当該ウイルス自体や「メールの添付ファイルの開封」や「メール本文のリンク先にアクセス」といった感染原因は必ずしも新規性を有するものではない。ここで新規性を有するのは，メール受信者に真正の（つまり，サイバー攻撃ではない）メールと誤信させて「メールの添付ファイルの開封」や「メール本文のリンク先にアクセス」をするよう仕向けるメールの送信方法なのである。ウイルスの特徴や感染原因に着目すれば新規性を有しないとしても，こうしたメールの送信方法が新規のものであれば，脅威に対する予見は困難といえる。

b．周知媒体の種類

新たな情報セキュリティ上の脅威が発見された場合，(i)ウイルス対策ソフトウェア会社等の専門性を有する会社がその旨をサイト上で公表する，(ii)当該脅威に起因する情報漏えい事件が報道される，(iii)公的機関（主にIPA）が当該脅威についての注意喚起をそのサイト上で公表する，というのが一般的な流れであると思われる。北海道警察捜査情報漏えい事件の第二審判決は，「ウイルス対策ソフトを扱う会社等一部のサイトに掲載されるにとどまっており，同月29日の京都府警における捜査情報の流出の記事が出るまで，一般にはアンティニーGの内容が広まってはいなかったこと」を考慮のうえ，予見可能性を否定しており，周知性の観点からは(i)では足りないとしたものである。他方で，unico個人情報漏えい事件（**12月号Ⅱ 1(3)**）は，SQLインジェクションの脅威について「経済産業省及びIPAが，ウェブアプリケーションに対する代表的な攻撃手法としてSQLインジェクション攻撃を挙げ，……SQLインジェクション対策をするように注意喚起をしていたことからすれば，その事態が生じ得ることを予見することは容易であったといえる」としており，これは，周知性の観点から(iii)をもって足りるとするものである。

したがって，周知媒体としては，(i)では足りないものの，(iii)は十分であるとして，問題は(ii)の扱いである。いまのところ参考とすべき裁判例はないものの，周知媒体は，あくまで周知性を基礎づける一要素という位置付けからすると，報道の大きさや報道からの期間との相関関係から周知性は判断されることになると思われる。

c．一定期間の経過

周知性を認定するあたり，脅威が初めて確認されてからの期間の経過も大きな判断要素となる。北海道警察捜査情報漏えい事件および愛南町個人情報流出事件は，ともにファイル共有ソフトに関するウイルスに起因する情報漏えいが問題となった事案である。前者では，ウイルス対策を講じる会社のサイトにおいて当該ウイルスの存在が公表された時点（平成16年３月23日頃）から情報漏えいの時点（同月29日または30日）まで，わずか１週間程度しか経過していなかったことが考慮されて予見可能性が否定されたのに対して，後者では，情報漏えいが平成19年４月30日に発生していたものであるため，特に期間に触れることなく端的に周知性を認めて予見可能性を肯定している。

(イ) 結果回避義務

① 他の結果回避措置の存在

結果回避義務の検討にあたっては，他の結果回避措置の存在が重要な指標となる。すなわち，他のセキュリティ対策をとっていれば，サイバー攻撃を回避できたのではないか，という文脈で他の結果回避措置の存在が検討される。

リモートアクセスを利用した不正アクセスにより個人情報が漏えいした事案であるYahoo！BB顧客情報えい洩事件（**11月号Ⅱ1(1)(ウ)**）の第二審判決は「ユーザー名とパスワードによる認証以外の例えばコールバック機能等の規制措置を採るべきであったか」，不正アクセスをした者が在職中に「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」とした。SQLインジェクションというサイバー攻撃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unico個人情報漏えい事件は「バインド機構の使用又はエスケープ処理を行うことで，本件流出という結果が回避できた」とし，他の結果回避措置の存在をあげた。

② 他の結果回避措置をとることのコスト

ただし，企業にとってサイバーセキュリティの確保は当然費用を要するものであり，経営判断として費用対効果[2]を考慮せざるをえない。他の結果回避措置が存在する場合，当該措置を採用する場合のコストも当然考慮される。すなわち，他の結果回避措置が存在するからといってただちに結果回避義務違反が認められるわけではない。

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，結果回避義務に関してというよりは一般論としてではあるが「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

[2] 岡村久道「コンピュータウイルス感染による個人情報えいと損害賠償責任」NBL813号33頁は，「結果回避義務を履行したといえるためには，必ずしも使用可能な対策すべてを講じなければならないわけではない。どのような対策を選択すべきか，どの程度の対策を講じれば足りるかについては，外部流出を回避すべき対象情報の性質・量，脅威の種類・程度，各対策を使用することの難易度・有効性等を総合して決せられるべきものであろう」とする。

キュリティ対策を取ることが必要というべき」と判示する。

また，上記のunico個人情報漏えい事件は，「バインド機構の使用又はエスケープ処理を行うことで，本件流出という結果が回避できたところ，本件ウェブアプリケーションの全体にバインド機構の使用又はエスケープ処理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」いとして，他の結果回避措置を採用するにあたって要する労力や費用を考慮した。

事後的にみて結果を回避するための手段があったとしても，当該手段を採用するための労力や費用が著しく大きい場合にまで結果回避義務違反が肯定されるわけではない。

(3) 使用者責任

情報システムの開発・保守の全部または一部を外部のシステム開発受託者に委託することは少なくない。また，システム開発受託者においても，委託内容の規模や難易度に応じて，さらにシステム開発再受託者に再委託することも一般的である。

こうした情報システムの開発・保守に伴い，個人情報の取扱いをも委託する場合，個人情報保護法22条は，「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」とし，さらに，同条を具体化した個人情報の保護に関する法律についてのガイドライン（通則編）は，「委託元が委託先について『必要かつ適切な監督』を行っていない場合で，委託先が再委託をした際に，再委託先が不適切な取扱いを行ったときは，元の委託元による法違反と判断され得る」とする。

仮に自社以外の従業員の過失に起因して個人情報が漏えいした場合，どこまで使用者責任を負うかという点で，裁判例上，指揮監督関係の有無が主要な争点となる。

この点につき，契約関係がなくても，実質的に一方が他方を指揮監督する（すべき）関係があれば使用関係は認められるという点に争いはない。

そのうえで，実質的な指揮監督関係の有無を判断するにあたって裁判例上以下の要素が参考になる。

(ア) 報告，協議の存在

宇治市住民基本台帳データ漏えい事件（**11月号Ⅱ 1(1)(ア)**）の第二審審判決は，実質的な指揮監督関係を認定するにあたり，システム開発再受託者のアルバイト従業員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）を指摘した。

同様に，TBC事件（**11月号Ⅱ 1(1)(エ)**）の第二審判決は，実質的な指揮監督関係を認定するにあたり，個人情報取得者がシステム開発受託者から随時「運用に関する報告」を受けていたこと（報告の存在）および「障害や不具合が発生した」場合には，システム開発受託者と原因や対応等について「協議」していたこと（協議の存在）を指摘した。

(イ) 作業場所

宇治市住民基本台帳データ漏えい事件の第二審判決は，実質的な指揮監督関係を認定するに当たり，上記の協議の存在のほか，個人情報を持ち出したシステム開発受託者の従業員が個人情報取得者の庁舎内で作業を行っていたという事情（作業場所）を指摘した。

報告，協議の存在および作業場所は，いずれも使用者と被用者との間に物理的に指揮監督の機会があったことを示すものである。

(ウ) 重要な決定権限の所在

TBC事件の第一審判決は，実質的な指揮監督関係を認定するにあたり，上記の協議および報告の存在のほか，個人情報取得者に「本件ウェブサイトの具体的内容の決定権限」

（決定権限の所在）があったことを指摘し，同様に同事件の第二審判決は，個人情報取得者たる「控訴人は，本件ウェブサイトのコンテンツの具体的な内容を自ら決定し」ていたことを指摘した。

(エ) 専門的技術的知識の欠如

他方で，システム開発を委託した側に専門的技術的知識が十分でない場合，指揮監督関係の認定にあたって消極的影響を及ぼすか。具体的には使用者責任を問われた個人情報取得者から「十分な専門的技術的知識がないので，専門的技術的知識を有するシステム開発受託者を指揮，監督することは不可能」との主張がなされることがある。

この点について，TBC事件の第一審判決は，「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」個人情報取得者「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ず，その委託された業務には独立した判断や広い裁量はなかったものと認められるから，指揮，監督関係を否定することはできない」とした。

3 おわりに

全４回にわたって，企業法務の観点から，サイバーセキュリティに関する企業の責任を紹介した。

企業の責任とあわせて役員の責任について問題となるところであるが，紙面の都合上，今回は触れることができなかった[3]。

サイバーセキュリティは，技術的な側面が強い分野であるが，セキュリティ上のインシデントが発生した場合の企業の法的責任に鑑みると，社内における個人情報の管理，情報システムの開発を委託するにあたっての契約上の留意点，委託先企業の管理監督など，法務が果たすべき役割は小さくない。

サイバー攻撃の多様化・大規模化という攻撃側の事情に加え，今後IoTの普及により企業側としてもサイバーセキュリティの確保を不可欠とする領域が益々拡大する。

企業のサイバーセキュリティの確保・向上にあたり，本連載が少しでも役に立てれば幸いである。

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。

[3] 役員の責任については，拙稿「情報漏えいと取締役の情報セキュリティ体制整備義務」中央ロー・ジャーナル14巻３号（2017年内刊行予定）を参照されたい。