

## 情報システム障害・事故における IT 事業者の責任

東京地判平 26. 1. 23 判時 2221 号 71 頁

弁護士法人 内田・鮫島法律事務所  
伊藤 雅 浩

### I. 事案の概要等

原告は、インテリア商材の卸小売及び通信販売等を行う株式会社であり、被告は、情報処理システムの保守受託等を行う株式会社である。原告は、平成 21 年 2 月 4 日、被告に対し、原告のウェブサイト（本件ウェブサイト）における商品のウェブ受注システム（本件システム）の導入を委託した。被告は本件システムを完成させて納入し、原告は、平成 21 年 4 月 15 日、本件ウェブサイトの稼働を開始した。本件ウェブサイトでは、当初、顧客のクレジットカード情報を保存していなかったが、平成 22 年 1 月に被告は、原告の依頼を受けて本件システムを変更し、顧客のクレジットカード情報（カード会社名、カード番号、有効期限、名義人、支払回数及びセキュリティコード）が、本件システムのデータベースに保存される仕組みとなった。ただし、クレジットカード情報は暗号化されていなかった。原告と被告との間には、本件ウェブサイトの保守に関する契約が締結されていた。

平成 23 年 4 月、本件システムのサーバに不正アクセスがあり、顧客のクレジットカード情報を含む個人情報が流出した。セキュリティ会社の調査によると、SQL インジェクション攻撃という手段<sup>1</sup>により、当時サーバ内に保有されていたクレジットカード情報 6975 件全件が漏えいした可能性があるということであった。

原告は、被告に対し、被告が適切なセキュリティ対策を執っていなかったなどと主張し、委託契約の債務不履行に基づき損害賠償金約 1.1 億円を請求した。

被告は、これに対し、債務不履行の有無や、損害の額を争うとともに、「契約金額の範囲内において」支払うという損害賠償責任制限規定の適用を主張した。

### II. 判旨

原告の請求の一部である 2200 万円余りの損害賠償及び遅延損害金について認容した（確定）。

---

<sup>1</sup> セキュリティ上の不備を攻撃する手段の一つ。プログラムが想定しないデータベース操作命令 (SQL 文) を実行させることにより、データの改ざんや取り出しが可能になる。

## 1. 債務不履行の存否について

「被告は、平成21年2月4日に本件システム発注契約を締結して本件システムの発注を受けたのであるから、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認められる。そして、本件システムでは、金種指定詳細化以前にも、顧客の個人情報を本件データベースに保存する設定となっていたことからすれば、被告は、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解すべきである。」

「経済産業省は、平成18年2月20日、「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」と題する文書において、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ことから、独立行政法人情報処理推進機構（以下「IPA」という。）が紹介するSQLインジェクション対策の措置を重点的に実施することを求める旨の注意喚起をしていたこと、IPAは、平成19年4月、「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」と題する文書において、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文の組み立てにバインド機構を使用し、又はSQL文を構成する全ての変数に対しエスケープ処理を行うこと等により、SQLインジェクション対策をすることが必要である旨を明示していたことが認められ、これらの事実に照らすと、被告は、平成21年2月4日の本件システム発注契約締結時点において、本件データベースから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いえることができる。

そうすると、本件ウェブアプリケーションにおいて、バインド機構の使用及びエスケープ処理のいずれも行われていなかった部分があることは前記2のとおりであるから、被告は上記債務を履行しなかったのであり、債務不履行1の責任を負うと認められる。」

## 2. 損害賠償責任制限の合意の成否等について

### (1) 損害賠償責任制限の合意の成否

「被告は、本件基本契約は、25条で当事者双方が民法の原則どおり損害賠償義務を負うことを確認し、29条2項で被告が損害賠償義務を負う金額を制限したものであると主張する。

そこで検討するに、本件基本契約は、第9章で「損害賠償その他」について規定し、「第29条〔損害賠償〕」として、「乙（注：被告）が委託業務に関連して、乙又は乙の技術者の故意又は過失により、甲（注：原告）若しくは甲の顧客又はその他の第三者に損害を及ぼした時は、乙はその損害について、甲若しくは甲の顧客又はその他の第三者に対し賠償の責を負うものとする。」（1項）、「前項の場合、乙は個別契約に定める契約金額の範囲内において損害賠償を支払うものとする。」（2項）と定める一方で、第7章で「機

密保持」について規定し、「第19条〔秘密保持義務〕」として、「甲、乙は、「対象情報」を厳に秘匿し、相手方の事前の書面による承諾なく、これを第三者に開示若しくは漏洩してはならない。」(1項)、「第25条〔損害金〕」として、「甲若しくは乙が本契約内容に違反した場合には、その違反により相手方が被る全ての損害を賠償するものとする。」を定めている。

以上の規定を合理的に解釈すれば、本件基本契約は、29条2項で、被告の原告に対する損害賠償金額を原則として個別契約に定める契約金額の範囲内とし、25条は、29条2項の例外として、被告が対象情報を第三者に開示又は漏洩した場合の損害賠償金額については制限しないことを定めたものと解するのが相当である。」(下線は筆者。以下同じ。)

## (2) 賠償額上限条項の適用

「原告は、被告に重過失がある場合には、本件基本契約29条2項は適用されないと主張するので検討する。

本件基本契約29条2項は、ソフトウェア開発に関連して生じる損害額は多額に上るおそれがあることから、被告が原告に対して負うべき損害賠償金額を個別契約に定める契約金額の範囲内に制限したものと解され、被告はそれを前提として個別契約の金額を低額に設定することができ、原告が支払うべき料金を低額にするという機能があり、特に原告が顧客の個人情報の管理について被告に注意を求める場合には、本件基本契約17条所定の「対象情報」とすることで厳格な責任を負わせることができるのであるから、一定の合理性があるといえる。しかしながら、上記のような本件基本契約29条2項の趣旨等に鑑みても、被告(略)が、権利・法益侵害の結果について故意を有する場合や重過失がある場合(その結果についての予見が可能かつ容易であり、その結果の回避も可能かつ容易であるといった故意に準ずる場合)にまで同条項によって被告の損害賠償義務の範囲が制限されるとすることは、著しく衡平を害するものであって、当事者の通常の意味に合致しないというべきである(売買契約又は請負契約において担保責任の免除特約を定めても、売主又は請負人が悪意の場合には担保責任を免れることができない旨を定めた民法572条、640条参照。)

したがって、本件基本契約29条2項は、被告に故意又は重過失がある場合には適用されないと解するのが相当である。」

## (3) 重過失の有無

「被告は、情報処理システムの企画、ホームページの制作、業務システムの開発等を行う会社として、プログラムに関する専門的知見を活用した事業を展開し、その事業の一環として本件ウェブアプリケーションを提供しており、原告もその専門的知見を信頼して本件システム発注契約を締結したと推認でき、被告に求められる注意義務の程度は

比較的高度なものと認められるところ、前記のとおり、SQLインジェクション対策がされていないならば、第三者がSQLインジェクション攻撃を行うことで本件データベースから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、バインド機構の使用又はSQL文を構成する全ての変数に対するエスケープ処理を行うこと等の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。また、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く、本件流出という結果を回避することは容易であったといえる。

そうすると、被告には重過失が認められるというべきである。」

上記のように述べて、本件基本契約29条2項（賠償額の制限規定）の適用はないとし、相当因果関係ある損害について賠償責任を認めた（ただし、過失相殺により3割減額）。

### III. 検討

#### 1. はじめに

2014年7月、ベネッセから数千万件の個人情報が流出したという事件は、大きく報道された。消費者庁「平成25年度個人情報の保護に関する法律施行状況の概要」<sup>2</sup>によれば、同年度中に事業者が公表した個人情報の漏えい事案は366件であり、そのうち、漏えいした人数が50,001人を超える件数が18件を占める。近時は、大規模な漏えい事故が多く発生しているが、こうした事故発生時の事業者の法的責任に関する裁判例はそれほど多くない。

この種の事故が発生した場合における紛争類型として、本人から個人情報取得事業者に対する不法行為（プライバシー侵害等）に基づく損害賠償請求類型<sup>3</sup>と、個人情報取扱事業者から委託先のIT事業者に対する債務不履行等に基づく損害賠償請求類型<sup>4</sup>がある。本件は、消費者から個人情報を集めた通信販売業者（原告）が、そのシステムの保守を委託していたIT事業者（被告）に対して損害賠償を求めたというものであり、後者の類型にあたる。

<sup>2</sup> <http://www.caa.go.jp/planning/kojin/pdf/25-sekou.pdf>

<sup>3</sup> このような事例として、東京高判平19.8.28判タ1264号299頁（TBC事件）、大阪高判平19.6.21（平18(ネ)1704号。Yahoo!BB事件）、大阪高判平13.12.25平13(ネ)1165号（住民基本台帳事件）などがある。

<sup>4</sup> このような事例として、本件のほか、東京地判平21.12.25（平20(ワ)19890号）などがある。なお、いずれの類型にも分類しがたいが、クレジットカード決済代行会社から、サイト運営事業者に対して、クレジットカード情報の漏えい責任を追及した事例として東京地判平25.3.19（平23(ワ)39121号）がある。

個人情報漏えい事故は、事案によって、発生原因・態様や、事故後の対応、発生した被害の状況や事業者の規模などが様々である上、IT 事業者と委託者との契約内容も様々であり、法的責任の判断に関する一般的な定式というものは存在しない。本件は、IT 事業者の負っていた義務の内容と違反の有無、損害の額、責任限定条項の解釈など、様々な争点について判断がなされているが、あくまで特定の状況下での事故についての判断に過ぎない。しかしながら、本判決の意義を検討することは、契約実務、紛争対応に意義があると思われるため、以下、順に検討していく。

## 2. セキュリティ対策と債務不履行

### (1) 問題の所在

一般に、個人情報の取扱いを含むシステム保守にかかる契約は、事務の取扱委託を内容とするものであるから、準委任契約に分類される。そのため、IT 事業者は善管注意義務（民法 656 条、644 条）を負うことになるが、義務の違反が認められるか否かは、個人情報の取扱いの委託を受けた IT 事業者と委託者との合意内容次第である。ところが、委託者・IT 事業者間で、SLA<sup>5</sup>と呼ばれる具体的なサービスレベルの合意がなされているケースは必ずしも多くなく、事故が発生してはじめて専門家として負うべき義務の内容及びその程度が争われることになる<sup>6</sup>。

### (2) 関連裁判例

システム保守業務の委託を受けた事業者が負うべき義務の内容として判断した事例として、前掲注 4 の東京地判平成 25 年判決がある。この事例は、何者かの不正アクセスによりクレジットカード情報が漏えいした事例であるが、決済代行業者（原告）と、クーポンサイト運営事業者（被告）との間に、「契約者は、会員のカード情報及びX社決済システム（略）を第三者に閲覧、改ざん又は破壊されないための措置を講じるとともに、契約者のサイトを第三者に改ざん又は破壊されないための措置を講じる」との定めがあった。原告告間に、取るべきセキュリティ対策の項目に争いがなかったものの、その程度については争いがあった。裁判所は、この点について、「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。そして、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

<sup>5</sup> Service Level Agreement の略。IT サービスの製品やサービス内容の機能、範囲、性質、性能などの合意をいう。一般社団法人電子情報技術産業協会(JEITA)では、「民間向け IT システムの SLA ガイドライン」を公表しており、日経 BP 社から第 4 版(2012)が出版されている。同ガイドラインにはセキュリティサービスの項目として、ウィルス対策、不正アクセス検出・防止等が挙げられている。

<sup>6</sup> 善管注意義務は、受任者の職業・地位・知識等において一般的に要求される平均人の注意義務であり、各具体的場合の取引の通念に従い相当と認むべき人がなすべき注意義務をいうとされる（新版注釈民法(16)・225 頁（中川高男執筆））。

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、クレジットカードの情報という機密性の高い情報を扱わない通常のウェブサイトと比べると、費用を要する高度のセキュリティ対策を実施すべきものというべきである。」とした上で、特別なセキュリティ対策をとっていたという主張立証はないとして被告の債務不履行を認めた。

前掲注4の東京地判平成21年では、被告は、原告に対して「善良な管理者の注意をもって管理する義務を負っていた」としたうえで、P2Pファイル交換ソフト<sup>7</sup>がインストールされたパソコンがウィルスに感染したことによって流出したという事実を摘示し、債務不履行を認めた。

また、本人からの不法行為に基づく請求の事例ではあるが、前掲注3の東京高判平成19年では、被告の委託先（履行補助者）が、IT専門事業者であり、その技術的水準として、「個人情報を含む電子ファイルについては、一般のインターネット利用者からのアクセスが制限されるウェブサーバーの「非公開領域」に置くか、「公開領域」（ドキュメントルートディレクトリ）に置く場合であっても、アクセスを制限するための「アクセス権限の設定」か「パスワードの設定」の方法によって安全対策を講ずる注意義務があった」にもかかわらず、適切な対応がなかったことを理由に、履行補助者の過失を認めて不法行為責任を認定した。

以上のとおり、セキュリティ対策に関する義務内容及びその程度は、事案によって異なるため、一般化することは困難である。しかしながら、情報漏えいという結果が発生した場合において、結果的に事業者の義務違反を否定したという事例はなく、特にクレジットカード情報等の機密性の高い情報を取り扱う場合には、事故発生当時にとり得る範囲での高度なセキュリティ対策が求められるといえる。

### （3） 本判決

本判決では、平成18年当時に経済産業省から「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」という文書において、SQLインジェクション攻撃について注意喚起をし、独立行政法人情報処理推進機構がこれを受けて具体的な対策を公表していたという状況に照らし、原被告間で契約が締結された平成21年2月の時点で、当時一般的に知られていたSQLインジェクション攻撃の対策措置を講じたプログラムを提供すべき義務を負っていたとした。

他方で、原告は、善管注意義務の内容として、被告がクレジットカード情報を暗号化する義務を怠ったとの主張もしていたが、平成19年当時の厚生労働省・経済産業省「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」において、暗号化等の措置については、いずれも「望ましい」という程度にとどまっていたことから、契約で特別に合意していない場合でも当然に義務を負っていたとは認められな

---

<sup>7</sup> インターネットを介してサーバを経由することなく不特定多数の利用者とのファイルをやり取りするためのソフトウェアをいう。

いとした。

義務の内容、程度については、いずれも当時一般に知られていたガイドライン等の公的文書、客観的情報に基づいて一般的な IT 事業者が当然に有すべき義務の水準を認定したものであって、適切なものであったといえる。換言すれば、個人情報を取り扱う事業者は、業界内に一般的に知られているセキュリティ情報を収集し、必要な対策を取ることが求められる。

### 3. 責任制限規定の適用範囲

#### (1) 問題の所在

本件では、被告が負うべき賠償責任の範囲を巡って、原被告間で合意された下記の責任限定条項（2項）が適用されるべきかが争われた（下線は筆者）。

##### 第29条〔損害賠償〕

- 1 乙が委託業務に関連して、乙又は乙の技術者の故意又は過失により、甲若しくは甲の顧客又はその他の第三者に損害を及ぼした時は、乙はその損害について、甲若しくは甲の顧客又はその他の第三者に対し賠償の責を負うものとする。
- 2 前項の場合、乙は個別契約に定める契約金額の範囲内において損害賠償を支払うものとする。

IT 事業者が締結する契約の多くには、このように契約金額を賠償額の上限とする責任限定契約が設けられている。ソフトウェアの不具合、情報漏えい、データ消失などの重大な障害が発生した場合には、委託者の事業に深刻な影響が生じかねないが、そのような損害すべてについて IT 事業者が賠償責任を負わせることになると、得られる報酬との均衡を失することにもなりかねない。経済産業省「情報システム・モデル取引・契約書」<sup>8</sup>の53条においても、このような趣旨のもとで損害賠償額の上限規定が置かれている。

この種の規定そのものの有効性は否定しがたいだろう<sup>9</sup>。しかし、消費者契約法8条1項2号及び4号では、事業者の故意又は重過失による場合の損害の一部を制限する条項を無効としている。事業者間の契約においても、故意又は重過失の場合（特に重過失の場合）に賠償の範囲を制限する規定が効力を有するかどうか問題になる。

#### (2) 関連裁判例等

##### ア. 重過失免責に関するもの

宝石会社の代表者がホテルに宝石入りバッグを預けたところ、何者かにバッグが盗難されたという事例において、ホテルの宿泊約款における責任限定条項について「故意又は重大な過失がある場合にまで責任制限規定が適用されるのは著しく衡平を害するもの

<sup>8</sup>平成19年4月に「情報システムの信頼性向上のための取引慣行・契約に関する研究会」から公表されたモデル契約書とその解説。

<sup>9</sup>（2）イで述べるように、東京地判平16.4.26も、責任限定条項自体の合理性は認めている。

であって、当事者の通常の意味に合致しない」とした事例がある<sup>10</sup>。

また、前述の消費者契約法のほか、商法 581 条（物品運送）、同 739 条（海上運送）、鉄道営業法 11 条の 2 などにおいては、重過失の場合における事業者の責任限定を排斥している<sup>11</sup>。

このように、一定の契約類型においては、法律上、責任制限規定の有効性が限定されているほか、特段の法的規制がない類型においても、当事者間の交渉が予定されていない約款においては、重過失の場合においても責任を限定すべき合理性がない場合には、重過失の場合には責任制限規定を適用しないという限定解釈がなされるものと考えられる。

## イ. 賠償額の上限に関するもの

IT 事業者を受託者とするシステム開発業務委託契約書中の「委託金額を上限として」賠償するという規定に関して判断した事例として、東京地判平 16.4.26(平 14(ワ)第 19457 号)がある。裁判所は、当該条項自体は、「一般論としては、コンピューターのプログラムに不具合が存在した場合、その損害がときには莫大な額になる危険の存することからすれば、その危険のすべてを請負人側に負わせることを防ぐ趣旨において、合理性のあるもの<sup>マ</sup>の思われ、よって、本件において、そのすべてが、信義誠実の原則（民法 1 条 2 項）及び公平の原則に照らし、また、民法 90 条に違反し、無効であると言いうる事情は認められ<sup>マ</sup>ない」とした。しかし、委託金額は 500 万円であったものの、結果的に 8500 万円程度の作業量に膨れ上がったという事情を考慮し、低廉すぎる金額で契約が締結されたという場合には、これを賠償額の上限とすることは信義公平の原則に反するとして、「作成しようとしていたシステムの出来高を上限」という限度で有効と解すべきと判断した。

賠償額の上限についても、その額が著しく低廉である場合など、当事者の合理的意思に反すると評価すべき場合には、相当な額を上限とするような解釈がなされる可能性がある。

### (3) 本判決

原被告間の契約は、免責規定に関する法定の制限がかかる類型ではなく、また、交渉の余地がない約款でもなかった。しかし、本判決は、賠償額の上限を定めた前述の責任限定条項について、委託者である原告が支払うべき料金を低額にするという機能があることなどを理由に、一定の合理性があるとした。しかし、重過失がある場合にまでも、賠償範囲を制限することについては「著しく衡平を害するものであって、当事者の通常

<sup>10</sup> 最判平 15.2.28 判時 1829 号 151 頁

<sup>11</sup> 合意の有効性、解釈の事例ではないが、書留郵便物について、郵便業務従事者の故意又は重大な過失による不法行為についてまで免責又は責任制限を認める規定は憲法 17 条に反し、無効だとした判例がある（最大判平 14.9.11 民集 56 卷 7 号 1439 頁）。



の意思に合致しない」とした。その根拠として、担保責任の免除特約があっても悪意の場合には排除されるとする民法 572 条, 640 条を挙げている<sup>12</sup>。これらの条文は、「知らなから告げなかった」とあるように、故意の場合の免責を排除するのみであって、「重大な過失によって知らなかった場合も同様とする。」といった規定になっていたわけではない。裁判所が、売買、請負の一般的な規定を根拠に、重過失の場合における責任限定条項は適用されないという限定解釈を行った点に特徴がある。

#### 4. 重過失の意義

##### (1) 問題の所在

上記のように、重過失の場合には責任限定条項が適用されないとすると、重過失と軽過失の区別が重要になってくる。同じ注意義務違反であっても、「重過失」と評価される場合には、相当因果関係ある損害全てについて賠償責任が生じ、「軽過失」の場合には、免責あるいは責任範囲が限定されるからである。

重過失とは、一般に、注意義務違反の程度が甚だしい過失をいい、各種の法令で多く使用されている用語であるが<sup>13</sup>、具体的にどの程度の注意義務違反があれば重過失と評価されるのかは明確ではない。

##### (2) 関連裁判例等

重過失の意義に関するリーディングケースとして、しばしば援用されるのが、失火責任法但書における「重大ナル過失」の意義について述べた最判昭和 32 年 7 月 9 日民集 11 卷 7 号 1203 頁である。裁判所は、「重大な過失とは、通常人に要求される程度の相当な注意をしないでも、わずかの注意さえすれば、たやすく違法有害な結果を予見することができた場合であるのに、漫然これを見すごしたような、ほとんど故意に近い著しい注意欠如の状態を指すものと解する」とした（下線部は筆者）。これによれば、故意と同視できる程度の限定的な場合のみを指すものと考えられる。

さらに、証券取引所のシステム障害等に伴う損害賠償請求事件<sup>14</sup>において、証券取引所への参加者契約における「重大な過失」の解釈について、裁判所は、前記最高裁判例を次のように敷衍して述べた。

「重過失（重大な過失）について、判例（最高裁昭和 32 年 7 月 9 日判決・民集 11 卷 7 号 1203 頁）では「ほとんど故意に近い著しい注意欠如の状態」と表現し、「ほとんど故意に近い」とは「通常人に要求される程度の相当な注意をしないでも、わずかな注意さえすれば、たやすく違法有害な結果を予見することができた」のに「漫然とこれ

<sup>12</sup> 判決文ではあくまで「参照」として条文を挙げただけである（II.2.（2））。

<sup>13</sup> 「重大な過失」という表現が用いられている例として、民法 95 条（錯誤）、商法 17 条（商号譲受人の責任）、会社法 429 条（役員等の第三者に対する損害賠償責任）、特許法 102 条（損害の推定）、消費者契約法 8 条（事業者の損害賠償の責任を免除する条項の無効）など。

<sup>14</sup> 東京高判平 25.9.24 判タ 1394 号 93 頁

を見過ごした」場合としている。これは、結果の予見が可能であり、かつ、容易であるのに予見しないである行為をし、又はしなかったことが重過失であると理解するものである。これに対して、重過失に当たる「著しい注意欠如の状態」とは著しい注意義務違反、すなわち注意義務違反の程度が顕著である場合と解することも可能である。これは、行為者の負う注意義務の程度と実際に払われた注意との差を問題にするものである。前者のような理解は重過失を故意に近いものと、後者のような理解は重過失を故意と軽過失の中間にあるものと位置付けているようにも解される。」

前掲最判昭和 32 年は、「ほとんど故意に近い」と「著しい注意欠如の状態」とを特に分けて論じているわけではないので、上記のように2つの基準、類型に分けて論じることについて十分な説明がなされているとは言い難い。しかし、前掲最高裁判例が過失を主観的な側面で捉えていたのに対し、専門家や事業者にとっての過失とは客観的注意義務状態であるという近時の理解に基づいて、重過失の要件を、結果予見可能性・容易性があり、かつ、結果回避可能性・容易性がある場合であると解しているものと思われる。

### (3) 本判決

本判決では、特段の説明もなく、重過失の意義について、「重過失がある場合（その結果についての予見が可能かつ容易であり、その結果の回避も可能かつ容易であるといった故意に準ずる場合）」とした。この点は、前掲東京高判と同様に解している。さらに、SQLインジェクション攻撃については、当時の技術常識に照らして予見可能かつ容易であり、これに対する対策は可能であり、困難だという事情もないことから容易であるとしたうえで、被告の重過失を認めた。

専門事業者である IT 事業者には客観的な基準に基づく注意義務が要求されると考えられる。したがって、重過失を、前掲東京高判平成 25 年と同様に客観的過失の考え方に基づいて解釈することが適切だといえる。

## 5. まとめ

本稿では、本判決を題材に、情報漏えい事故発生時における IT 事業者の債務不履行の有無と、責任限定条項の限定解釈、重過失の意義について取り上げた。本判決は、特定の事故における特定の契約条項の元での事例判断に過ぎない。しかし、IT 事業者が取るべきセキュリティ対策と法的義務の関係や、責任限定条項の有効性・限定解釈など、多くの事例において問題となり得る争点について裁判所の判断を示したものであって、今後の実務上の参考となる事例だといえる。なお、そのほかにも、損害の額・種類や、委託者側の落ち度（過失相殺の割合）について実務上関心が高いところである。本件でも多様な損害項目について、相当因果関係の有無等が、争われたが、紙幅の都合上、割愛した。