

東京地判平成 26・1・23 判例時報 2221 号 71 頁  
ウェブサイトによる商品の受注システムを利用した  
顧客のクレジットカード情報が流出した事故につ  
き、システムの設計、製作、保守等の受託業者の債  
務不履行に基づく謝罪・問合わせ等の顧客対応費  
用、売上損失等の損害賠償責任が肯定された事例

遠藤 元一

## I 事実の概要

インテリア商材の卸小売、通信販売等を行う X（原告）は、情報処理システムの企画、保守受託及び顧客サポート業務、ホームページの制作、業務システムの開発等を行う Y（被告）との間で、X のウェブサイト（以下「本件ウェブサイト」という）における商品のウェブ受注システム（以下「本件システム」という）の設計、保守等の委託契約を締結し、本件システム稼働後、X は、Y との間で、本件ウェブサイトで顧客が利用したクレジットカード種別を X の基幹システムに送信する仕様（以下「金種指定詳細化」という）に変更する委託契約を追加して締結し、Y は本件システムに金種指定詳細化の機能を組み入れ、X は検収を経て本件システムを稼働させた。

それ以降、顧客が本件ウェブサイトでクレジットカード決済を行う場合、クレジットカード情報が本件システムを稼働させるために Y が利用していた外部業者のサーバーに入力され、同サーバーとカード会社との間でクレジットカード情報のやり取りが行われるようになったが、顧客のクレジットカード情報が暗号化されずにデータベースに保存される設定となっていた。

平成 23 年 4 月、本件サーバーに外部から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する事態が生じた（以下「本件流出」という）。セキュリティ会社の報告書によると、SQL インジェクション攻撃が断続的に行われたことが確認されると共に SQL インジェクションに対する脆弱性があったこと、当時保有していたカード情報 6795 件全件が漏洩した可能性が高いとされていた。

そこで、X は、Y が金種指定詳細化のために製作したアプリケーションが脆弱であったことにより本件ウェブサイトで商品の注文をした顧客のクレジットカード情報が流出し、顧客対応等が必要となったために損害を被ったとして、Y に対し、委託契約に関して様々な債務不履行を主張し、その債務不履行に基づき損害賠償金 1 億 0913 万 5528 円及び遅延損害金の支払を求めた。

## Ⅱ 判 旨

本件の争点である①本件流出原因及び程度、② Y の債務不履行責任の有無、③ X の過失と因果関係の断絶、④損害、⑤損害賠償責任制限の合意の成否等のうち、本稿で検討する②、④、⑤を中心に判旨を整理し、検討する。

### 1 本件流出原因及び程度（論点①）

・顧客のクレジットカード情報が暗号化されずに本件データベースに保存される設定となっていたこと、平成 23 年 4 月、本件サーバーに外部から不正アクセスがあり本件流出が発生したことに加えて、同月 20 日、クレジットカード

ド会社 2 社が、X からクレジットカード情報が流出した疑いがあると判断して警告を行ったことから、平成 23 年 4 月 20 日までに本件流出が発生したと認定した。本件ウェブアプリケーションには、SQL インジェクションに対する脆弱性があること、攻撃者はデータベース構造が分からないため、SQL インジェクション攻撃を悪用してデータベース構造の把握を行い、データベース情報を窃取するのが一般的であるが、ログ調査の結果およびクレジットカード情報の不正利用が 4 月 14 日から同月 20 日の間、増加したこと等の事実から、平成 23 年 4 月 14 日までに本件データベースの情報を窃取するために SQL インジェクションによる事前調査が行われ、更に同日に SQL インジェクション攻撃（データベースシステムを不正に操作する方法）が成功し、クレジットカード情報が読み取られたことが推認され、他に本件流出の原因が認められないことも考慮して、本件流出の原因は、4 月 14 日の SQL インジェクション攻撃であると認定し、「本件流出により漏洩した情報の内容及び件数は正確には分からない」が、最大でクレジットカード情報が 7316 件、クレジットカード情報を含まない個人情報が 9482 件漏洩した可能性が存するということになるとして上限数を認定した。

## 2 Y の債務不履行責任の有無（論点②）

・(1) Y は、X との間で、本件基本契約を締結した上で、個別契約として、本件システムの製作、保守サービス、クレジット情報の把握（金種指定詳細化）、本件ウェブサイトのデザイン変更作業（本件ウェブサイトメンテナンス契約）等にかかる本件個別契約を締結したのであるから、個別契約ごとに、当該個別契約及び本件基本契約に基づく債務を負う（本件基本契約 2 条により個別契約には本件基本契約が適用される）とし、また、

本件基本契約及び本件個別契約は別の時期に締結され、個別契約ごとに内容も異なるので、本件個別契約に基づき発生する債務を一体として把握することはできないとして、本件基本契約と各個別契約を全て一体の契約としてみるべ

きであるとの X の主張を排斥した。

・(2) 本件流出の原因は SQL インジェクションと認められるから、本件個別契約及び本件基本契約に基づき、Y に債務不履行 1、3 及び 5 が認められるかを検討し、債務不履行 1 の責任を負うと判示した。

ア 債務不履行 1（適切なセキュリティ対策が採られたアプリケーションを提供すべき債務の不履行）

Y 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、Y は、当該個人情報の漏洩を防ぐために必用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。

①経産省は、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」と題する文書で、IPA（独立行政法人情報処理推進機構）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、② 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」と題する文書で、ウェブアプリケーションに対する代表的な攻撃方法として 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に照らすと、Y は、平成 21 年 2 月 4 日の本件システム発注契約締結時点で、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。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り、Y は債務不履行 1 の責任を負うと認められる。

Y は、予見可能性がなかったと主張するが、SQL インジェクション対策を講じていなければ、第三者が SQL インジェクション攻撃を行うことにより本件データベースから個人情報が流出し得ることは Y において具体的に予見可能であって、それを超えて、個別の侵入態様を予見できなかったとしても、債務不履行 1 に係る Y の予見可能性が否定されないと判示した。

#### イ 債務不履行 3（カード情報を保存せず、保存する場合は暗号化すべき債務の不履行）

X は、金種指定詳細化業務に基づき、当然に、クレジットカード情報を本件サーバーおよびログに保存せず、保存しても削除する設定とし、又はクレジットカード情報を暗号化して保存すべき債務を負っていたと主張するが、裁判所は、厚労省及び経産省が平成 19 年 3 月 30 日に改正した「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」（同日厚労省・経産省告示第 1 号）では、クレジットカード情報等について特に講じることが望ましい安全管理措置として、利用目的の達成に必需最小限の範囲の保存期間を設定し、保存場所を限定し、保存期間経過後適切かつ速やかに破棄することを例示し、IPA は、同年 4 月、前記「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」と題する文書で、データベース内に格納されている重要なデータや個人情報については暗号化することが望ましいと明示していたことが認められる。しかし、上記告示等は、いずれも上記対策を講じることが「望ましい」と指摘するものにすぎないし、暗号化の設定内容等は暗号化の程度によって異なり、それによって Y の作業量や代金も増減すると考えられることに照らすと、契約で特別に合意していなくとも、当然に、Y がクレジットカード情報を本件サーバー及びログに保存せず、もしくは保存しても削除する設定

とし、又はクレジットカード情報を暗号化して保存すべき債務を負っていたとは認められないとした。

ウ 債務不履行5（Yによるセキュリティ対策の程度についての説明義務違反）

Xは①SQLインジェクション対策を講じていないこと、②セキュリティ対策が脆弱であること、③本件サーバに係るY・サーバー保有者間のレンタルサーバー契約では最低のセキュリティレベルの内容であること、④金種指定詳細化の際に、クレジットカード情報を暗号化せずに保存する設定になっていたことを主張したが、裁判所は、①QLインジェクション対策を講じていないことが債務不履行に当たるのであるから、それとは別に、信義則上の義務としてSQLインジェクション対策を講じていないことの説明義務は生じない、②主張を裏付ける証拠がない、③本件システムの脆弱さが本件流出に寄与したことを認めるに足る証拠がない④Xのシステム担当者は、Yからの説明で、セキュリティ上はクレジットカード情報を保存しない方が良く、そのほうが一般的であることを認識していたことが認められ、Yはクレジットカード情報の保存による危険性を説明したといえるとして、説明義務違反はなく、債務不履行5の責任は認められないとした。

### 3 Xの過失と因果関係の断絶・過失相殺（論点③）

Yは、因果関係の断絶論（①本件システムは運用当初、本件データベースに顧客のクレジットカード情が保存されていなかったが、Xの都合により本件データベースに顧客のクレジットカード情報が保存されるように仕様を変更した、②安全性及び改善の方法等に関してYが費用と改善方法を指摘したのに本件データベースに顧客のクレジット情報が保存される仕様を変更しなかったなどの行為で、Yの債務不履行と本件流出との間の因果関係が断絶された）を主張したが、裁判所は、①について、「金種指定詳細化は、クレジットカード

情報を含まない顧客の個人情報の流出とは無関係であるから、クレジットカード情報の流出の関係でのみ因果関係が断絶するか否かが問題となる」として、債務不履行 1 と本件流出との因果関係が断絶は認められないとし、②については、「通常は本件データベースに保存されているクレジットカード情報を第三者が見ることはできず、本件流出によりクレジットカード情報が流出したのは、SQL インジェクション対策を怠るという Y の債務不履行 1 による危険が現実化したものであり、その認識した後 X が Y に対して本件データベース上のクレジットカード情報を保存しない設定とし、又は暗号化することなどを指示しなかったことは、本件流出の発生という結果を招来したのではなく、Y の債務不履行 1 と本件流出の発生との条件関係を否定するものではなく、因果関係を断絶するものと解することはできない。」とした。

さらに、顧客のクレジットカード情報のデータがデータベース上にあり、セキュリティ上はクレジットカード情報を保有しない方が良いことを認識し、Y から本件システム改修の提案をうけていながら、何ら放置していたことは、クレジットカード情報の漏洩の一因となったことは明らかであるから、3 割の過失相殺をするのが相当であるとし、上記の過失相殺事由は、因果関係の断絶を基礎づける事実として、当事者が十分な攻撃防御をしているから、過失相殺をすることは弁論主義に反せず、当事者への不意打ちともならないと判示した。

#### 4 損害について（論点④）

X が損害として主張した、①本件ウェブ受注システム委託契約関連して支払った代金、②顧客への謝罪関連費用（① QUO カード及び包装代、②お詫びの郵送代、③お詫び郵送に係る資材費及び作業費、④告知郵送費用、⑤告知の封筒代、⑥お詫びのメール配信の外注費、⑦お詫び呼び QUO カードの書留郵便代）、③顧客からの問い合わせ等の対応費用、④調査費用、⑤データセンター使用料、⑥事故対策会議出頭交通費、⑦リクナビネクスト応募フォーム変更、⑧売上損失のうち、②～⑦の損害項目については、④について本件流出の原因



等という専門的知見を必要とする作業を個人情報の漏洩という性質から早急に行うために専門的知見を有する業者 2 社を起用して行った調査費用は相当性を欠くとはいえず、Y に対する損害賠償を行うために必要な費用として合理的な範囲にとどまるとの説示を加えている他は、特に具体的な説示をすることなく Y の債務不履行と相当因果関係のある損害として、概ね X の主張した金額を損害として認定している。問題は、本稿が検討する①、⑧であり、①は X が主張する合計 2074 万 1175 円のうち 27 万 5625 円、⑧は売上損失 6041 万 4833 円のうち 400 万円を認定したにとどまる。

(1) 本件ウェブ受注システム委託契約に関連して支払った代金については、Y の債務不履行により本件流出が生じたため、新たなウェブ受注システムに変更せざるをえなくなり、本件ウェブ受注システム委託契約に基づき支払った代金相当額の損害を被ったとして、本件個別契約の代金合計 2074 万 1175 円が損害との X の主張に対し、裁判所は、X は、本件ウェブサイトが稼働を開始した平成 21 年 4 月 15 日から野村総合研究所のサーバーおよび Y とは別の会社のアプリケーションを利用したウェブサイトに移行した平成 23 年 8 月 23 日まで、Y との契約に基づき提供された本件ウェブアプリケーション等のサービスによる利益を享受していたのであるから、Y に債務不履行があったからといって、本件個別契約に基づき支払った代金が当然に損害となるものではない。ただし、X は同年 9 月以降は Y による保守サービスを受けず、本件サーバーの利用をしていなかったのであり、同月以降に支払った保守サービス料及びサーバー利用料相当額の利益は享受していないと認められ、X がサーバー及びアプリケーションを変更したことは、Y の債務不履行を受けて必要となった措置というべきで、平成 24 年 2 月から平成 24 年 1 月分の保守サービス料及びサーバー利用料として前払いした 63 万円のうち平成 23 年 9 月分から平成 24 年 1 月分の合計 27 万 5625 円（63 万円×5 月/12 月×消費税 1.05）は Y の債務不履行と相当因果関係のある損害と認められる」として、27 万 5625 円を認めた。

(2) 売上損失については、平成 23 年 4 月 21 日から同年 8 月 22 日までイン



ターネット上の商品販売においてクレジットカード決済機能が利用できなくなった期間にインターネット上で商品を販売できていれば、少なくとも 6041 万 4833 円を売り上げることができたとの X の主張に対し、裁判所は、X の具体的な売上減少を明らかにする決算書類等は提出されていない以上、X の損害額を認定する際には、売上減少に伴って支出を免れた仕入れ原価相当額を控除する必要があるが、本件ウェブサイトでは多様な商品が販売され、売上げが減少した商品ごとの仕入れ原価を立証することは困難であるため、4 ヶ月の売上損失としては 400 万円の限度で Y の債務不履行と相当因果関係のある損害とした（民訴 248 条）。

(3) Y の債務不履行と相当因果関係のある損害は合計 3131 万 9568 円であり、3 割の過失相殺をして 2262 万 3697 円と認定した。

## 5 損害賠償責任制限の合意の成否等（論点⑤）

本件基本契約第 9 章「損害賠償その他」には、29 条[損害賠償]として、Y が委託業務に関連して、Y 又は Y の技術者の故意または過失により、X 若しくは X の顧客又はその他の第三者に損害を及ぼした時は、Y はその損害について、X 若しくは X の顧客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、Y 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)との規定が、第 7 章「機密保持」には、19 条[機密保持]として、X、Y 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との規定が、25 条[損害金]として、X 若しくは Y 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との規定がある。本件流出により流失した個人情報、クレジットカード情報は、機密保持条項の「機密情報」の要件を満たさないことから、第 1 に、上記の規定の関係、解釈(X は 29 条の責任制限特約が情報漏洩の場合にも適用されると主張)、第 2 に、責任制限特約が適用されるとして重過失がある場合に 29 条 2 項が適用されるか、

第3にYに重過失が認められるか等が争点とされた。

本判決は、第1については、29条の規定と25条の規定について合理的解釈として、「25条は、29条の例外として、Y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、「29条2項は、損害賠償その他について規定した第9章内に定められており、損害賠償に関する総則的規定と解される」とした。第2については、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恐れがあることから、損害賠償金額を個別契約に定める契約金額の班内に制限したものと解され、Yはそれを前提として個別契約の金額を定額に設定することができ、Xが支払うべき料金を定額にするという機能があり、特にXが顧客の個人情報の管理についてYに注意を求める場合には、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、一定の合理性があるが、Y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るといった故意に準ずる場合）にまで同条項によってYの損害賠償の範囲が制限されるところとは、著しく衡平を害するものであって、当事者の通常的意思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、29条2項は、Yに故意また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」とした。

第3については、Xが、Yの重過失の評価根拠事実として主張する、①電子商取引の設計・構築に当たってSQLインジェクション攻撃への対策を講じることは専門業者として当然であったこと、②Yは無償配布ソフトウェアEC-CUBEをベースとして本件ウェアアプリケーションを構築しており、誰でもEC-CUBEのプログラムの仕組みを知ることができ、第三者からの攻撃が容易であるため、Yは特にセキュリティ対策に中止すべきであったこと、③Yは、本件ウェブアプリケーション納品後もEC-CUBEのセキュリティ対策の修正プ

ログラム（パッチ）を適用し、又は X に適用を推奨すべきであったにもかかわらず、本件システムに上記パッチを適用していなかったこと、④ X と Y との間の契約実態が ASP であり、ASP 業者がアプリケーションソフトに関するセキュリティ対策を講じるのが通常であるため、X は Y がセキュリティ対策を行っていると誤信していたこと、⑤ Y は専門業者であるにもかかわらず、クレジットカード情報を本件データベースだけでなく、ログに記録する設定にしていたなど、本件システムに関するセキュリティレベルは極めて低いものであったこと、⑥ Y には本件システムのセキュリティ対策についての説明義務違反があることから、Y が賠償すべき金額を制限することは極めて不合理な結果となるため許されない等のうち、②③は証拠がなく、④～⑥は評価根拠事実と認められないとし（ただし、Y が専門業者であるという点は、Y の注意義務の程度を基礎づける要素となる）、①については、Y は、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、X 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、Y 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して、SQL インジェクション対策がされていなければ、SQL インジェクション攻撃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 Y において予見が可能であり、かつ、経産省及び IPA が、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（バインド機構の使用又はエスケープ処理を行うこと等）をするように注意喚起しており、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、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、本件で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して、Y には重過失が認められ、29 条 2 項は適用されないと判示した。

### Ⅲ 研 究

#### はじめに

インターネットを利用してウェブを通じて行う電子取引が広く浸透している現在、ネットを通じて機微情報・個人情報が流出・漏洩させる事案をめぐる法的紛争も増加しつつある。本判決は①本件流出原因及び程度、②Yの債務不履行責任の有無、③損害項目・金額、④Xの過失と因果関係の断絶・過失相殺、⑤責任制限特約の有効性の範囲<sup>1)</sup>等、様々な論点について興味深い判断を示しているが、紙幅の制約等から本稿は、上記②、③および⑤を取り上げて検討する。

#### 第1 Yの債務不履行責任の成否

##### 1 ソフトウェア開発の法的性質

本件は、瑕疵担保ではなく、債務不履行として論じられ、裁判所も債務不履行の有無として論じている。ところでソフトウェア開発契約の法的性質に関して裁判例では、表題に必ずしもとられることなく<sup>2)</sup>、請負契約と捉えるものが多く見られる<sup>3)</sup>。ソフトウェア開発契約の法的性質を確定することは法的問題を認知して処理する際の前提となる基礎事情を確定するという意味で有意と

---

1) 取引から発生する責任を免除し、あるいは一定の限度に制限する特約で、責任を免除する特約を「免責特約」、責任を制限する特約を「責任制限特約」ともいうが、両者を「責任制限特約」と総称する。大村敦志『消費者契約法[第4版]』（有斐閣、2011）186頁は責任制限条項を「相手方の責任を加重したり自己の責任を軽減するもの」と定義する。免責・責任制限条項（特約）一般については奥田昌道編『新版注釈民法（10）Ⅱ 債権（1）』（有斐閣、2011）209～255頁〔北川善太郎＝潮見佳男〕

2) 東京地判平成22・9・21判タ1349号136頁

3) 想定される契約類型としては、請負契約、準委任契約、売買契約、労働者派遣契約等があるが、請負契約か準委任契約かが争われることが多いとされている。

考えられる<sup>4)</sup> (本件契約は、仕事の未完成が争われているわけではないという意味では準委任契約か請負契約かを論じる必要はないが、法的性質を請負契約と捉えると債務不履行ではなく瑕疵担保として論じる局面が生じ、また、契約書に明記されていない論点を解決する際の指針を請負契約の規定に求めることになるという意味で法的性質を決定する意義がある)。そこで、以下、ソフトウェア開発契約の法的性質を検討する。

契約を区別する上で目安となるのは、誰がソフトウェア開発の完成責任(仕事完成義務)を負っているか、依頼を受けた側にどれだけの業務的独立性があるかであり<sup>5)</sup>、裁判例はユーザーが業務をシステム化するためにベンダーにソフトウェア開発を依頼する典型的な場合は請負であるとの判断枠組みを採っている。

X は Y に本件ウェブサイトの商品のウェブ受注システム(本件システム)の設計、保守等を委託し、稼働後には金種指定詳細化の仕様変更も委託し、Y は委託を受けた設計・開発・仕様変更等の業務を行うなど、Y は仕事完成義務を負っているのであるから、本件の契約の法的性質は請負契約と解すべきである。

この点、X は本件契約の法的性質につき請負契約ではなく委任契約と主張するが<sup>6)</sup>、これは Y が本件基本契約に基づく個別契約を請負契約として請負の瑕疵担保責任には基本契約 26 条 2 項が適用され、Y の責任期間は業務完了後

---

4) 潮見佳男『契約各論 I』10～11 頁、石川博康「典型契約と契約内容の確定」(内田貴・大村敦志編・民法の争点) 236 頁、小粥太郎「典型契約の枠組み」法律時報 1068 号 45 頁

5) 東京地方裁判所プラクティス委員会第二小委員会「ソフトウェア開発関係訴訟の手引」(以下「ソフトウェア訴訟の手引」として引用する) 判タ 1349 号 5 頁、田中俊次ほか大阪地方裁判所裁判官ら「ソフトウェア開発関連訴訟の審理」判タ 1340 号 8 頁

6) 判時 2221 号 79 頁、Y の主張は同 78 頁

1 年とする主張に対する反論という文脈でなされた主張である。26 条 2 項の文に照らしても Y の主張はもともと無理筋な主張であり、X がそれに振り回され、混乱した主張をした可能性があるように思われる。

## 2 債務不履行責任と瑕疵担保責任との区別基準

本件契約の法的性質を請負契約と捉えたと、次に、本件は債務不履行、瑕疵担保責任のいずれの局面での争点なのかが問題となる。請負建築に関する裁判例・学説の準則は、「予定されていた最後の工程までを終えているか否か」を債務不履行と瑕疵担保とを区分けする分岐点と捉え、最後の工程まで終えていない場合は仕事の未完成でありそれ自体は瑕疵ではないが、予定された最後の工程まで終了したが不完全なため修補を加える必要がある場合には仕事は完成したが目的物に瑕疵があると解すべきであり<sup>7)</sup>、最後の工程まで終えたか否かは客観的に判断されるべきで、取引通念や社会通念に従って判断される<sup>8)</sup>、というものである。

ソフトウェア開発契約についても、ソフトウェアには不具合はつきもので、それが全くない状態(完全無欠性)は物理的にも経済的にも実現は困難であり、それは完成後の瑕疵担保の問題で処理するという前提で、当初契約で予定していた最後の工程まで終えたか否かを基準として終了後は瑕疵担保が適用されるとするのが裁判例の主流の考え方と解されている<sup>9)</sup>。そして、ソフトウェア開

---

7) 東京高判昭和 36・11・20 高民集 14 巻 10 号 730 頁、東京高判昭和 47・5・29 判時 668 号 49 頁、東京高判昭和 61・5・28 判時 1194 号 82 頁。内山尚三「新版注釈民法 (16)」(有斐閣、1989) 119 頁、内山尚三・山口康夫『叢書民法総合判例研究 請負 [新版]』(一粒社、1999) 138 頁、滝井繁男『逐条解説 工事請負契約約款 (四訂 新版)』(酒井書店、1994) 216 頁

8) 東京地判平成 3・6・14 判時 1413 号 78 頁

9) 東京地判平成 14・4・22 判タ 1127 号 161 頁、東京地判平成 22・1・22LLI/DB、東京地判平成 22・12・27、東京地判平成 25・9・30、東京高判平成 26・1・15 (いずれも判例集未掲載)。前掲注 5) ソフトウェアの手引 14 頁

発の標準的な工程では検収の終了により運用に移行するため、原則として検収を経て引渡しを受けた段階で仕事の完成を認めてよいと考えられる<sup>10)</sup>。検収・引渡しを基準として債務不履行と瑕疵担保を区分けすることで、瑕疵担保責任の期間制限の起算点（民法 637 条 1 項）も明確になる。

本件のアプリケーションソフトは、X の検収を経て本件ウェブサイトにもインストールされた時点<sup>11)</sup> 以後は瑕疵担保責任が適用される。

ところで、本判決は、瑕疵担保責任ではなく、債務不履行責任と捉えて、具体的な債務不履行を観念して攻撃防御が行われているが、では債務不履行責任ではなく、瑕疵担保責任として論じるとしたら、債務不履行として論じている本判決と比べ、判決の結論に相違が生じるか、ということ実は瑕疵担保責任の問題として議論する場合でも、次に述べるとおり、本判決の債務不履行の存否をめぐる判断と同様の論理を辿って瑕疵の存否を判断することになり、結論的にも本判決と決定的な相違が生じることはないと思われる<sup>12)</sup>。

なぜなら、請負人は、性能、品質、規格等において契約に適合した仕事を完成させる義務を負っている。そして、瑕疵とは、契約で明示的に合意されている内容をベースとしながら、それだけでなく、契約の性質、契約の目的、契約締結に至る事情その他の事情によって決まると解される。この瑕疵を契約の趣旨を踏まえて目的物が有するべき性状を確定した上で、完成された目的物が当該あるべき性状に適合しているか否かについて判断されるが、これは、売買の瑕疵担保責任（民法 570 条）に関する最高裁判決の主観的瑕疵概念と同じ判断

---

10) 東京地判平成 16・12・22 判タ 1194 号 171 頁は交付があった以後は瑕疵担保責任が適用されるとする。

11) DVD などの記録媒体に記録した上で納品される場合はその納品の時点

12) 三村量一元裁判官が法的評価をどちら（債務不履行か瑕疵担保か）にするかによって結論がそれほど変わるとは考えていないと発言し、実務家も賛意を表明している。三村量一・上山浩・桶田大介「情報システムの開発・運用と法務」NBL 1050 号 11 頁。



枠組みである<sup>13)</sup>。

瑕疵を判断する場合、契約内容に適合するか否かは、売買の目的物に契約当事者が与えた共通の意味を探究し、それに従って契約適合性が判断され、次いで、両当事者の共通の理解が明らかでないときは契約の解釈により当事者が合理的に考えれば理解したと認められる通常の意味に従って契約に適合しているか否か判断することになるから<sup>14)</sup>、これは契約の解釈と同じ判断枠組みに従うことになる。したがって、瑕疵の判断も債務不履行の判断も、契約の解釈という同じ判断枠組みに従って瑕疵あるいは債務不履行の存否が決まることになると考えられるからである。そこで、以下では判旨が採る債務不履行構成を前提とした本判決の判示の意義・問題点等を論じる。

### 3 セキュリティ対策を講じたアプリケーションを提供すべき義務の黙示の合意による認定について

・(1) 本判決は、Xが主張した5つの債務不履行と本件流出の原因とを結び付けて、本件流出原因がSQLインジェクションによる場合につきXは債務不履行1、3、5を主張するものと主張整理を行い、債務不履行1（ネットワークやサーバーのセキュリティ対策を講ずべき債務の不履行）を認め、債務不履行3（カード情報を保全せず、保存する場合には暗号化すべき債務の不履行）、債務不履行5（Yによるセキュリティ対策の程度についての説明義務違反）の主張は排斥した。

・(2) 上記で最も検討を要するのは発注当時の技術水準に沿ったセキュリティ対策を施したソフトウェアを提供することがX・Y間で黙示的に合意されて

---

13) 最判平成22・6・1民集64巻4号953頁、最判平成25・3・22判時2184号33頁

14) 潮見佳男「売買・請負の瑕疵担保責任」NBL1045号8頁

いたとしたうえで、債務不履行 1 を認定するとともに、債務不履行 3 を否定したことが合理的・説得的な説示になっているかである。

本件とは異なる論点ではあるが、商法 509 条の諾否通知義務について、下級審裁判例は、学説の議論とは異なり、基本的商行為か否かに拘らないが、かといってあまり同条の適用範囲を広く認めているわけでもなく、申込の内容が合理的な条件であるか等の要素を勘案し、当該申込に対する沈黙が承諾を意味すると当然に予想される取引類型である場合に限って商法 509 条の適用を認める傾向を看取することができる<sup>15)</sup>、すなわち商法 509 条の適用範囲を契約の成立の効果が遡って考察するアプローチを採っていると評価できると解することができるが、このアプローチを突き詰めていくと、商法 509 条の有無にかかわらず、黙示の承諾についての事実認定に極めて近接していく。

商法 509 条の適用に見られる黙示の合意に等しい契約解釈の手法は、申込を受けて沈黙を保っている当事者に申込に対する応諾の意思表示を認める、つまり申込者により提示された条件による契約の成否を画定する役割を果たすにとどまる。

これに対しソフトウェア開発の仕様の契約適合性が争点とされる場合は、明示の合意の有無を検討し、それが無い場合に黙示の合意（あるいは合理的意思解釈）を検討することになるが<sup>16)</sup>、明示の合意の有無の認定が純粹の事実認定の作業が中心となるのに対し、黙示の合意の事実認定は、システムの要件定義書、基本設計書等の仕様内容を超えて、合意の中にいかなる内容を補充し、含意の取扱いをするかという多分に評価の要素を伴う作業である<sup>17)</sup>。黙示の

---

15) 東京地判昭和 52・4・18 判時 850 号 3 頁、東京高判昭和 58・9・28 判時 1092 号 112 頁等 江頭憲治郎『商取引法〔第七版〕』（弘文堂、2013）10 頁、11 頁注 3

16) 司法研修所『民事訴訟における事実認定—契約分野別研究（製作及び開発に関する契約）—』（法曹会、2014）158 頁

17) 司法研修所・前掲注 16) 136 頁

合意というのは、裁判所の最終的な規範的な解釈として合意を認定するものであって、信義則などの一般条項と同様（あるいはそれ以上）に融通無碍に使われるリスクがある。

黙示の合意があったというだけでは、結論を述べているに等しく、判旨に説得力があるか否かは、黙示の合意の認定する事情や論理として明確かつ合理的なものを提示できているかによって決まる。本判決は、適切なセキュリティ対策を採ったアプリケーションを提供すべき債務（債務不履行1）は、黙示の合意に含まれるが、カード情報を保存せず、保存する場合に暗号化すべき債務（債務不履行3）は明示の合意がないと認定できないと判示するが、債務不履行3を否定する論拠と対比して、果たして合理的・説得的な説示と言えるかが問題となる。

本判決は、①厚労省及び経産省が平成19年3月30日に改正した「個人情報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」（同日厚労省・経産省告示第1号）では、クレジットカード情報等について特に講じることが望ましい安全管理措置として、利用目的の達成に必需最小限の範囲の保存期間を設定し、保存場所を限定し、保存期間経過後適切かつ速やかに破棄することを例示し、IPAは、同年4月、前記「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」と題する文書で、データベース内に格納されている重要なデータや個人情報については暗号化することが望ましいと指摘するに過ぎないこと、②IPAの文書でも、データベース内のデータ全てを暗号化の処理を行うとサーバー自体の負荷になるため暗号化の範囲について考慮が必要であり、暗号化の設定内容等によって作業量や代金も増減するから、契約で特別の合意が必要であることの2つを理由とする。

しかしながら、①については、厚労省・経産省告示第1号は、クレジットカード情報について必要最小限の範囲の保存期間の設定・保存場所の限定・保存期間経過後適切かつ速やかに廃棄すること、要するにクレジットカード情報を必要最小限を超えて保存しないことを「特に講じることが望ましい」と強調して

いる。

本判決は、債務不履行 1 の認定に際しては、経産省の文書に QL 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があり、IPA の文書に 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を論拠としており、それと比較すると、債務不履行 1 は黙示の合意内容に含まれ、債務不履行 3 が黙示の合意の内容に含まれないという帰結をもたらすだけの決定的な相違とは思われない。また、②については、債務不履行 1 では、「セキュリティ対策は、コスト面や実用面との相関関係で対策レベルが検討されるべきものである」との X の主張に対し<sup>18)</sup>、サーバーに対する負荷、作業量や代金について何ら触れることなく、黙示の合意を認定しておきながら、他方、債務不履行 3 では、債務を否定する根拠としてサーバーに対する負荷をかけすぎないよう暗号化の設定内容等が様々であることや作業量や代金の増減を理由として持ちだすことは些か説得力を欠くように思われる。

仮に、X 代理人が、データや個人情報全ての暗号化ではなく、クレジットカードの暗証番号や個人情報のうち個人の識別可能性を困難にするような情報のみを暗号化することが Y の債務であるとして、その場合のサーバーに対しさほど負荷がかからないこと、作業量や代金の増額がそれほどの負担にならないことを主張・立証したと仮定したら、裁判所も、上記のような理由のみで債務不履行 1 を認め、債務不履行 3 を否定するとの結論を採ることに逡巡するのではなかろうか。本判決の説得性を高めるには、合意の欠缺を補充する拠り所を見出す必要がある。

(3) ではどのように考えるべきか。学説では、黙示の合意（意思表示）の認定に関して、当事者間の合意の欠缺を、慣習、任意規定、条理・信義則に従って

---

18) 判時 2221 号 76 頁

補充する、あるいは仮定的当事者意思（当事者が交渉によって合意していたとすれば、いかなる内容で空白部分を補充したか）を信義則による補充的契約解釈によって具体的に推認することによって補充することが行われ得ることが説かれている<sup>19)・20)</sup>。

この問題を考えるには、建築請負契約における瑕疵の判断枠組みに関する名古屋地方裁判所に所属する裁判官らによる研究成果として公表された論稿に示された考え方が参考になるように思われる<sup>21)</sup>。

同論稿によると、建築請負契約における瑕疵の判断枠組みは、第1に、目的物に当事者間の明示又は黙示の合意による契約内容に合致しない設計施工がなされていることが瑕疵とされる。ここでは、目的物の現状が契約内容に反するか否かが瑕疵の成否に関する唯一の基準であり、現状が建築基準法等に適合しているか否かは問題とされない。

第2に、契約内容に直接違反する場合でなくても、一般的建築基準を下回る設計施工がなされ、目的物の機能や耐久性等実質的な支障を来す場合は、①建築請負契約が、建築知識に疎い一般の注文者には直ちに理解困難な内容を含む専門的技術的性格を有していること、②請負目的物の存在・内容が近隣住民の安全・衛生等にも影響を与えること等から、瑕疵に該当することが認められる。

---

19) 河上正二『民法総則講義』（日本評論社、2007）255頁

20) 法務省民事局参事官室が作成した「民法（債権関係）の改正に関する中間試案の補足説明」（以下「中間試案・捕捉説明」として引用する）第29（契約の解釈）は、29・3で補充的解釈として仮定的当事者意思を採るが、当事者の仮定的な意思を事後的に認定することが実務的に困難である、法律行為の内容が不確定な場合にはその法律行為は無効であるという原則との関係も十分整理する必要があるとの指摘、当事者の仮定的意思に従って解釈することが実務的にも学説上も確立したものとして受け入れられているわけではないとの指摘があり、仮定的当事者意思については慎重な検討を求める意見が求められることが指摘されている。同注2文。

21) 青山邦夫・夏目明徳「工事の瑕疵」『住宅紛争の処理の実務』（判例タイムズ、2003）

ただし、目的物の機能や耐久性等の実質的な支障を回避するには当然に費用の増加を伴い、その費用の増加を注文者に負担させることを契約の解釈等によって認めることまではなされないため、一般的建築基準に違反する瑕疵と捉える場合には、技術水準と代金との緊張関係についても適切な考慮を払う必要がある。そこで、①建築実務に携わる者にとって一般的な建築基準になっており、一般に請負人が通常の代金中にこれを織り込んでいると理解できる場合か、②安全、衛星等の見地から必要最小限の基準であって、代金額のいかんにかかわらず、遵守されるべき建築基準と考えられる場合に限り、その違反が瑕疵になると解すべきであるとされる<sup>22)</sup>。

本件のようなソフトウェアの瑕疵（債務不履行）の判断に上記の考え方を参照すると、①ソフトウェアの設計・構築に携わる者にとって、一般的なソフトウェア設計・構築基準になっており、一般的にソフトウェアの設計・構築代金に織り込んでいる（あるいは織込むべきもの）と理解できるか否か、②安全等の見地から必要最小限の基準として、代金額のいかんにかかわらず、遵守されるべき基準と考えられる場合には、それを黙示の合意として契約の仕様に読み込むか否かは別として瑕疵（債務不履行）に該当すると解すべきことになる。

そして、ソフトウェア開発では、要件定義書・基本設計書に明示されていなくても、㊶報酬と工期（システムの仕様に連動し、グレードに影響する）、㊷環境・制約条件等（設置場所、利用形態、既存システム、ユーザー業務を規制する法令等の環境や制約条件）、㊸ユーザーが要求する機能、㊹要件定義書、基本設計書に明示しづらい性質の情報（システムの操作性等）等が考えられ、表示の際の書面外の事情として表示行為を組成する要素となり得るとされる<sup>23)</sup>。

債務不履行 3 を否定する論拠として暗号化の設定内容等が様々であることや

---

22) 青山・夏目前掲注 21) 126、132～136 頁

23) 司法研修所・前掲注 16) 151～155 頁

作業量や代金の増減に言及しているとおり、本判決も、上記㊦の報酬や㊦の環境・制約条件等が念頭におかれていたのではないかと推測される。ソフトウェアの提供に際して、特に㊦の環境・制約条件等を考慮してその当時の技術水準に沿った最低限必要とされるセキュリティ対策を施すことを所与の前提としたうえで、適切なセキュリティ対策を採ったアプリケーションを提供すべき債務（債務不履行1）として、SQL インジェクション対策を施したソフトウェアを提供すべき債務までは認められ、それ以上に、カード情報を保全せず、保存する場合には暗号化すべき債務の不履行（債務不履行3）は、全ての情報を暗号化することはサーバーへの負荷、部分的な暗号化の場合はどの範囲を暗号化するかを特定し、作業料と代金の増額を伴うため、黙示の合意の内容とは認定できないとしたと理解することができようか。

#### 4 説明義務違反を認定していない点について

Ⅱ2(1)ウのとおり、本判決は、説明義務違反を認定していない。①SQL インジェクション対策を講じていないこと、②セキュリティ対策が脆弱であること、③本件サーバに係るY・サーバー所有者間のレンタルサーバー契約では最低のセキュリティレベルの内容であること、④金種指定詳細化の際に、クレジットカード情報を暗号化せずに保存する設定になっていたことのXの主張につき、①はセキュリティ対策を施したソフトウェアを提供すべき債務の不履行を認める以上、それとは別に信義則上の義務として①を認める必要がないとの説示は合理的であり、③は主張を裏付ける証拠がないとの理由で排斥したことも当然である。これに対して、②の本件システムの脆弱さが本件流出に寄与したことを認めるに足る証拠がないことを理由に説明義務を否定する論法は、結論をもって理由とする循環論法に陥っている。また、④がクレジットカード情報の保存による危険性を説明したことを説明義務違反の理由としている点も説得力がないように思われる。

さらに、周知のとおり、当事者間に専門的知見や情報等について大きな格差



があり、知見や情報で優位にある当事者は相手方に対し、信義則上の情報提供義務、説明義務が課されることは、不動産売買、投資契約、フランチャイズ契約等に関する裁判例でも多く見られる<sup>24)</sup>。ソフトウェア関連の裁判例でも、システムの仕様変更の申入れがシステムの不具合・障害の発生の可能性を増大させる場合、ベンダーはソフトウェア開発契約の付随義務として、その専門的知見・経験に照らし、ユーザーにこれを告知して説明する義務を負うと判示した東京高判平成 26・1・15 LLI/DB もある。本判決が説明義務違反を認定していないのは、Y には別の債務不履行 1 が認められるという本件の事情に依拠しており、本件の事案を超えて射程は及ばないことに留意する必要があると思われる。

## 第 2 損害論—特に本件ウェブ受注システム委託契約に関連して支払った代金及び売上損失について

ソフトウェアの不備に関連して発生する損害は、財産的損害<sup>25)</sup>、風評被害<sup>26)</sup>、

---

24) 学説では、「情報量」の格差を是正する情報提供義務と「情報分析力」の格差を是正する説明義務の区別が意識されている。横山美夏「説明義務と専門性」判タ 1182 号 22 頁、前掲注 20) 327～332 頁（付随義務及び保護義務）、340～346 頁（情報提供義務）、長野弁護士会編『説明責任』（ぎょうせい、2005）3～15 頁等

25) 本件流出と異なり、データが毀損する事案では、①データそのものの価値（東京地判平成 21・5・20 判タ 1308 号 260 頁。もっとも、広島地判平成 11・2・24 判タ 1023 号 212 頁はデータ自体の財産的価値を算定することは困難であり、データ消失を慰謝料の補完事由として斟酌すると判示する）、②データ復旧費用（旭川地判平成 11・6・30 交通事故民事裁判例集 32 巻 3 号 975 頁は交通事故によるパソコン損壊の事案でデータ復旧に要する人件費を損害と認定）、③データの再構築費用（裁判例では、肯定した東京地判平成 13・9・28 判例集未登載と否定した広島地判平成 11・2・24 前掲ともにある）等が考えられる。

26) 大阪高判平成 16・2・19 訟務月報 53 巻 2 号 541 頁、東京高判平成 15・5・21 訟務月報 53 巻 2 号 205 頁は生産者・販売者の提起した国家賠償請求で国の賠償義務を肯定

非財産的損害等様々な損害を観念することができるが、特に本件システムのようにネットワークに接続されるソフトウェアに不具合があると、その不具合から生じる損害はネットワークを通じて無限に連鎖する可能性が抽象的には予見可能であるという状況が生じる。ソフトウェアの不備に関連して生起する損害を当事者間でいかに適正に分配するかは困難な問題である。本判決が認定している損害は概ね妥当であるが、疑問な点もある。

# 1 本件ウェブ受注システム委託契約に関連して支払った代金及び売上損失以外の損害項目について

Ⅱ・4でみたとおり、②顧客への謝罪関連費用、③顧客からの問い合わせ等の対応費用、④調査費用、⑤データセンター使用料、⑥事故対策会議出頭交通費、⑦リクナビネクスト応募フォーム変更については、④について一定の制限を付したほかはYの債務不履行と相当因果関係のある損害として、概ねXの主張した金額を損害として認定した。

本判決の認定に従い債務不履行に基づく損害賠償と捉える場合はもとより、瑕疵担保責任としての損害賠償請求権と捉え、瑕疵修補とともにする損害賠償請求を請求することを想定すると、その場合の損害賠償の範囲は瑕疵があることから生ずる全損害（履行利益）であり<sup>27)</sup>、修補に関する費用として、修補費用自体のほか、工事に必要な調査・鑑定費用、解体費用、解体部分の処理費用等を含むとされ、当該工事中に目的物が使用できないことによる損害（代替建物の賃料、当該建物で行っていた営業の売上の低下）、瑕疵に基づく無形的損害（紛争解決のために労力を要したことや、生活上の不便、慰謝料）、解決に必要な弁護士費用等が認められるとされる。上記は建築請負工事の事案に関する損害項目であり、これをアプリケーションソフトウェアの提供という本事

---

27) 青山・夏目前掲注21) 142～144頁。半田吉信『契約法[第2版]』（信山社、2005）424～425頁は瑕疵惹起損害、瑕疵による逸失利益、信頼損害等を含むとする。

案に即して考えると、上記②～⑦が相当因果関係の範囲として認容されることは当然であるし、債務不履行構成における損害賠償と瑕疵担保構成における損害賠償とで、賠償される損害の範囲に相違は生じないと考えられる。

## 2 本件ウェブ受注システム委託契約に関連して支払った代金について

本判決は、Y の債務不履行により新たなウェブ受注システムに変更せざるを得なくなったとして X が損害として主張し、請求した本件ウェブ受注システム委託契約に基づき支払った代金相当額である 2074 万余円は、X が本件ウェブサイトが稼働した平成 21 年 4 月 15 日から平成 23 年 8 月 23 日（Y とは別のアプリケーションを利用したウェブサイトへの移行日）までサービスによる利益を享受していたことを理由に当然に損害にならないとした（ただし、前払いした保守サービス料及びサーバー利用料相当額のうち平成 23 年 9 月から同 24 年 1 月分は利益を享受していないとして、Y の債務不履行と相当因果関係のある損害と認めた）。しかし、この判示には次のような疑問があり、賛成できない。

第 1 に、売買の瑕疵担保責任に基づく損害賠償として瑕疵でバイクが全焼した場合、購入した商品が欠陥品である事案で購入費用全額を損害として賠償を認める裁判例がある<sup>28)</sup>・<sup>29)</sup>。債務不履行構成の場合はもちろん瑕疵担保責任構成の場合でも、請負の瑕疵担保責任は債務不履行責任の特則であるから、その損害の範囲が（法的性質について議論があり、損害賠償の範囲も区々とされている）売買の瑕疵担保責任の損害の範囲よりも狭いというのはバランスを欠い

---

28) 東京地判平成 15・1・28 判時 1829 号 90 頁、東京高判平成 20・5・29 判時 2033 号 15 頁

29) 損害賠償の範囲について明確に判示した判例は見当たらない。また、裁判例は①信賴利益に限定するもの、②売主の債務不履行ないし不法行為を構成することを理由に相当因果関係の範囲内の賠償を認めるもの、③②のような前提事情がないまま相当因果関係の範囲内の損害を認めるものに分かれている。判例・裁判例の分析につき遠藤元一「債権法改正と売買の瑕疵担保責任ルールの変更（前編）」ビジネスロージャーナル 2015 年 8 月号 121 ～ 122 頁

ているのではなかろうか。

第2に、その当時の技術水準に沿ったセキュリティ対策を施していないアプリケーションを提供するという重大な債務不履行が認められ、セキュリティの脆弱性がつかれてクレジットカード情報や個人情報流出・漏洩する危険性に晒されている以上、たまたま一定期間、クレジットカード情報や個人情報が流出・漏洩していなかったからといって、Xが本件ウェブアプリケーション等のサービスによる利益を十全に受けていたとは到底いえない。

「売買あるいは請負の目的物に瑕疵があるとして、買主または注文者が売主あるいは請負人等に対し建物費用相当額の損害賠償を請求する場合、買主等が当該建物の引渡しを受けて居住している居住利益を得ているとして、損益相殺等の対象として損害賠償から控除することが許されるか」という論点に関し、売買の目的物である新築建物に重大な瑕疵があり、これを建て替えざるを得ない場合に、当該瑕疵が構造耐力上の安全性にかかわるものであるため建物が倒壊する具体的なおそれがあるなど、社会通念上、建物自体が社会経済的価値を有しないと評価すべきものであるときには、居住利益を控除することを否定した最高裁判決（最判平成22・6・17判時2082号55頁）がでている。

この判例は買主が瑕疵の存在を認識していたか否かによって結論を異にするものではなく、また、判旨の射程は請負人の瑕疵担保責任に基づく損害賠償にも及ぶと解されている<sup>30)</sup>。

判旨の「重大な瑕疵」をどこまで広げるのか、本判決の事案をそれに比肩するものと捉えうかは検討を要することではあるが、Yから提供を受けたソフトウェアが安全性の見地から必要最低限のセキュリティ対策すら採られておらず、ハッカー攻撃に対し極めて脆弱で、攻撃されれば容易に情報が外部に流出し、企業価値を毀損するリスクに恒常的に晒されていたことを考えると、本判

---

30) 平成22年度最高裁調査官解説民事篇（法曹会）408頁〔武藤貴明〕、同ジュリスト判批1419号129頁

決のように、一定期間サービスの利益を享受していたことを理由として代金相当額を一切損害として認めないという説示は、相当性を欠いているといわざるを得ない。

しかも、本件流出が発生しても、ソフトウェアについては、専門技術情報は受注者（ベンダー）に偏在しており、発注者は専門技術情報を知らないか理解できないことが多い（専門情報の非対称性）うえに<sup>31)</sup>、不具合があることが判明した場合、その原因を究明するのは専門技術を有する者であっても、相当の期間やコストを要する（本件でも X が起用した 2 社による数か月の調査を要した）。本件流出の原因がセキュリティ対策の不備にあったことが判明した場合には、安全性という観点からの基本的な対策を講じなかった受注者との間の信頼関係は既に破綻しており、そのような破綻した受注者に対し、対策を講じることを求めることを発注者に期待することも困難である。

このように考えると、債務不履行による損害として代金相当額である 2074 万余円の賠償を認めた上で、使用利益相当額を控除するか否かを検討するのが適切である。

第 3 に、民法 635 条但書にもかかわらず、建物としての存在価値をなくすほどの重大な瑕疵がある場合には、注文者からの立替費用相当額の損害賠償請求を認容する判決がある。

すなわち、請負契約において目的物に瑕疵があり、そのために契約をした目的を達することができないときは、注文者は契約を解除することができ（民法 635 条本文）、目的物が建物その他の土地工作物である場合は解除できないとされている（同条ただし書）。但書の趣旨として、土地の工作物が目的物である場合に解除を認めると請負人の負担が大きくなることが挙げられるが、建物の瑕疵が極めて重大な場合には、工事が未完成であると認定することで瑕疵担保責任の対象ではなく、債務不履行として解除を認定する裁判例が少なからず

---

31) 司法研修所・前掲注 16) 10 頁

認められる。他方、最上級審の判例は建物としての存在価値をなくすほどの重大な瑕疵がある場合には、注文者からの立替費用相当額の損害賠償請求を認容する判例があり（最判平成 14・9・24 判時 1801 号 77 頁）<sup>32)</sup>、これは瑕疵の程度によっては、請負人が解除を認めたのと同様の負担を負うべき場合があることを前提としたものであるといえる<sup>33)</sup>。

上記判例は、注文者による損害賠償を認めるにあたり、建物の存在価値を否定し、取り壊しができることを前提とした説示をしていることに留意する必要がある。建物としての現有価値がないと評価される場合は、瑕疵がなかったとしたら有したであろう交換価値が賠償されるべき損害になるというべきであり、それを実現するための建替え費用相当額を損害として認めることは、建築費用を考慮に入れて交換価値が確定されることから、是認できるとする見解もある<sup>34)</sup>。

民法 635 条但書の明文がある場合にすら、建物を取り壊して建替え費用全額の賠償を認めるこの判例があることを考えると、その当時の技術水準に沿ったセキュリティ対策を施していないアプリケーションの提供はおよそ債務の本旨に従ったアプリケーションの提供とはいえず、重大な債務不履行が認められると評価でき、X には別の専門家によるアプリケーションの設計構築費用相当額の損害賠償が認められるべきである。

### 3 売上損失について

本件流出により 4 ヶ月間、インターネット上の商品販売でクレジットカード

---

32) この判例は実質的に民法 635 条ただし書を修正する判断を示したものの指摘もある。前掲注 20) 中間試案・捕捉説明 479～480 頁。建替えるしかないほどの重大な瑕疵のある建物については、請負契約の解除を認める余地があるとする見解もある。近江幸治『民法講義 V 2 契約法 [第 3 版]』（成文堂、2006）56 頁

33) 民法 635 条但書は必ずしも合理的な規律ではないため、改正条文案では削除されている。

34) 潮見佳男「請負の瑕疵担保責任の法的性質と損害賠償」『契約規範の構造と展開』（有斐閣、1991）252 頁

決済機能が利用できなくなり、その期間にインターネット上で商品を販売できていれば少なくとも 6041 万余円を売り上げることができたとの X の主張に対し、本判決は、①クレジットカード決済機能が利用できなかったことで一定の売上減少があったことは推認できるが、具体的な売上減少額を明らかにする決算書類等が提出されていないうえ、②売上減少に伴い支出を免れ仕入原価相当額等を控除する必要があるが、多様な商品が販売されていると推認でき、売上が減少した商品ごとの仕入原価等を立証することは極めて困難であることを理由に、民訴法 248 条を根拠として 400 万円の限度で債務不履行と相当因果関係のある損害があると判示している。

この判旨は当然のことながら、最判平成 20・6・10 判時 2042 号 5 頁を意識した判断になっている。最判平成 20・6・10 判時 2042 号 5 頁の判断枠組みをより一般化した規範命題とすると、「損害賠償請求訴訟において、損害額の立証が困難であったとしても、民事訴訟法 248 条により相当な損害額を認定しなければならぬ」と定式化することができ、裁判所は、この定式が行為規範としてだけでなく、評価規範として機能することも意識して審理・判断することが求められるようになっているからである<sup>35)</sup>。

民訴法 248 条を適用するための要件は、①損害が生じたことが認められる場合であること、②損害の性質上その額を立証することが極めて困難であること、③口頭弁論の全趣旨及び証拠調べの結果に基づくことであるが、①の「損害」に逸失利益が含まれるかについて学説上争いがあり、損害の文言解釈として逸失利益（消極的財産損害）を除外することに合理性はないから、これが含まれると解するのが多数説であり<sup>36)</sup>、本判決もこの多数説を採っている。②の「立証が極めて困難であるとき」とは原則的証明度を要求した場合に、原告が不当

---

35) 加藤新太郎「民事訴訟法 248 条の構造と実務」田原睦夫先生古希記念『現代民事法の実務と理論（下巻）』（きんざい、2013）1051 頁

36) 加藤新太郎「相当な損害額の認定」ジュリ 1166 号 107 頁



に不利益となり、損害賠償法など実体法の趣旨・目的にそぐわない結果を生じ、損害額を立証するために民訴 248 条による以外に代替的な立証手段方法もないときをいうと解されている。本件では、多様な商品を販売し、商品毎に仕入れ価格や利益率が異なること、季節や時期に応じて価格変動が生じる商品の場合では同じ商品でも、仕入価格や利益率が異なるため、個別損害の立証が困難であることから、この要件を満たすと考えられ、本判決が②の要件を満たすと判断して金額を認定したことは妥当である。

判旨から理解が困難な問題は、損害額としてなぜ 400 万円と認定したのかである。民訴 248 条により認められる損害の範囲について裁判例は、相当の損害額を認定する場合、損害額につき控え目な金額を相当とするのもやむを得ないという抑制的算定説<sup>37)</sup>、損害額につき合理的な根拠をもって実際に生じた損害額に最も近いと推測できる金額を相当とすべきであるとする合理的算定説<sup>38)</sup>、いずれとも言及しないものに分かれている<sup>39)</sup>。

相当な額という文言からいうと、証拠資料からこまでは確実に存在したであろうと考えられる範囲に抑えた額ではなく、合理的と考えられるなかで、実際に生じた損害額に近いと推測できる額と解すべきであり、合理的算定説が相当と考える。

本判決が上記のどの説を採ったかは明らかではないが、400 万円という金額の低さが抑制的算定説を採ったからなのか、X が決算書等を提出しないことが考慮されているのか等、判決書からは窺い知ることはいできない。

---

37) 大阪高判平成 18・9・14 判タ 1226 号 107 頁、名古屋地判平成 21・12・11 判タ 1330 号 144 頁等

38) 東京地判平成 19・10・26 判タ 1293 号 129 頁、名古屋地判平成 21・8・7 判タ 1330 号 247 頁等

39) 東京地判平成 21・6・18 判タ 1310 号 198 頁等。これが最も多数説のようである。

### 第 3 責任制限特約の適用範囲と重過失の認定

#### 1 契約の有効解釈

本判決は、本件基本契約 29 条 2 項と 25 条の規定の関係について、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する責任制限特約である 29 条 2 項が第 9 章（損害賠償その他）に定められていることから、損害賠償に関する総則的規定と捉え、25 条は「機密保持」に関して例外的に適用されるとして、25 条の「本契約内容に違反した場合」との記載は誤記で、「本章の規定に違反した場合」と読み替えるべきと判示した。契約の条項間に矛盾がある場合に、それぞれの条項を文言どおりに適用したり、直ちに一方を無効とするのではなく、合理的・整合的な解釈が可能かを探求して、可能であれば、そのような形で解釈することが、契約自由の原則により当該契約を締結した当事者の意思にも適う。本判決の判示は、このような契約の有効性を維持する解釈であり、正当である。

#### 2 責任制限特約が適用される範囲

本件基本契約 29 条 2 項の責任制限特約が有効であるとするが、特に X が顧客の個人情報の管理について Y 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として、重要情報については X の利益が擁護されていることを有効性の論拠としている点に特徴がある。約款論の不利益条項の議論を意識しているのであろうか。

本判決は続けて、主観的要件を設けていない 29 条 2 項は故意または重過失がある場合には適用されないこと、重過失とは、権利・法益侵害の結果についての予見が可能かつ容易であるといった故意に準ずる場合であると判示している点に重要な意義がある。

主観的要件により免責・責任制限特約はどこまで有効と解されるのか、また、本件基本契約のように主観的要件について何ら触れられていない場合はどのように扱われるかについての判例・裁判例をみると次のとおりである。

まず、債務者が故意の場合に責任を免責・制限する特約は、無効であるという判例法理が早くから確立している。

反対に、軽過失の場合に責任を免責・制限する特約は、具体的な事案との関係で無効とする若干の例外的な裁判例があるものの、それ以外は契約自由の原則、公序良俗、権利濫用に該当しないこと等を論拠として基本的には有効とする裁判例が多数存在している。つまり、軽過失に関する責任免責・制限特約は特段の事情がない限り有効と解するのが裁判例の水生的傾向と考えられ、学説でも同様に解されている。

では、重過失の場合の責任免責・制限特約はどうか。これを無効とする判例・裁判例がいくつかでており、責任免責・制限特約自体は無効としないものの故意・重過失がある場合は当該特約は適用されないとする判例もでている。学説は比較的最近まで重過失免責を認めるか否かにつき明言してこなかったが、今日では重過失免責は無効であるとの見解が多数説である。このような判例・裁判例および学説の状況下で、ある具体的な債務不履行・不法行為等の事象が生じた場合、その事案で故意・重過失が認められるかによって責任の成否が決まる。

そこで、そもそも重過失とはなにか、どのような判断枠組みで判断されるかという点が問題となる。

重過失の意義について、従来の判例は、「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の注意をしないでわずかな注意さえすれば違法有害な結果を予見することができた」のに「漫然これを見過ごした」場合としている（大判大正2・12・20民録19輯1036頁、最判昭和32・7・9民集11巻7号1203頁）<sup>40)</sup>。

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

---

40) 最判昭和51・3・19民集30巻2号128頁は「わずかな注意さえすれば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、著しく注意を欠如した結果、これを見過ごしたものの」とする。

行為を行い、または行わなかったことが重過失であると捉えるものである。

しかし、故意とも重なり得る失火の場合の重過失の規範を重過失が問題となる局面一般に通用する規範として捉えることは的確とはいえない<sup>41)</sup>。

他方、会社法 429 条 1 項の重過失について取締役の義務の程度を考えてそれとのかい離の度合いが著しいことと捉える判例もある<sup>42)</sup>。現在では、過失は、かつてのように結果が発生することを認識できたのに不注意でそれを認識しない心理状態（主観的過失）ではなく、行為義務違反、すなわち、なすべきことをしなかったこと（客観的過失）と解されており、裁判実務も同様の傾向、すなわち、違法有害な結果を予見認識しその結果を認容しあえて作り出す心理状態という故意とは異なり、過失は客観的な注意義務違反と捉えられている。

故意とのアナロジーとして重過失を抱える従来判例の立場では、積極的な心理状態である故意と客観的な注意義務の欠如の状態である過失とを「近い」ものとして説明することは相当に無理があることは否めない<sup>43)</sup>。さらに結果発生を予見できたが、実際に予見していなかった場合は、違法有害の結果をあえて作り出すという積極的な心理状態とはなりえないから、予見可能であるが予見していなかった者に重過失は認め難いという難点も生じる<sup>44)</sup>。

下級審裁判例は、形式的には上記の定義を用いながらも実際はこれとは異なるスキームで重過失を認定しているが（多くは重過失を「著しい注意義務違反」と捉えている<sup>45)</sup>）、これは最高裁の重過失の定義のもつ難点を回避するためと

---

41) 潮見佳男『不法行為法 I 〔第 2 版〕』（2009、信山社）305 頁、道垣内弘人「『重過失』概念についての覚書」『民法学における法と政策（平井宜雄先生古希記念）』（有斐閣、2007）537～539 頁

42) 最判昭和 44・11・26 民集 23 卷 11 号 2150 頁

43) 金判 1422 号 23 頁囲み枠、奥田編・前掲注 1) 221 頁参照 [北川＝潮見]

44) 吉田正夫「判批」ビジネスロージャーナル 2013 年 11 月号 49 頁

45) 潮見佳男『不法行為法』（1999、信山社）170 頁、奥田編・前掲注 1・211 頁 [北川・潮見] 223～240 頁

理解される。

誤発注控訴審判決（東京高判平成 25・7・24 金判 1422 号 20 頁）は、システムにバグがあり利用者に損害が生じたときのシステム提供者に適切に取消注文処理ができるシステムを提供する義務についての不完全履行を認めつつ、重過失の判断については重過失を「ほとんど故意に近い著しい注意欠如の状態」に基づき、①「ほとんど故意に近い」と②「著しい注意欠如の状態」に分けて、②に関して「著しい注意義務違反（重過失）」というためには、結果の予見が可能であり、かつ容易であること、結果の回避が可能であり、かつ容易であることが要件となる」として、具体的な事案について重過失を否定する注目すべき判断を示した。

ここでは、重過失を「著しい注意義務違反」と捉え、重過失を認定する要件（判断枠組み）として、結果の予見可能性・容易性、結果回避の可能性・容易性を要求し、従来の判例と異なる規範が示されている。

この枠組みは、①の「ほとんど故意に近い著しい注意欠如の状態」と②「著しい注意欠如の状態」との相違が明確でないなどの問題点が指摘されているものの<sup>46)</sup>、過失を客観的な注意義務違反と捉える最近の裁判実務の立場に立ちながら、重過失の意義・判断枠組みを構築するものであるで、今後の先例的な枠組みとなる可能性があり<sup>47)</sup>、注目される。

もっとも、極めて限られた範囲にすぎないが、複数の裁判例の分析から得られた知見を前提とすると、①「ほとんど故意に近い」という重過失概念のフォーミュラ自体には重過失か否かを決定する内実は含まれておらず<sup>48)</sup>、故意概念と連続性のある概念として重過失概念を観念することは的確とはいえない、

---

46) 吉田・前掲注 44) 49 頁

47) 弥永真生「判批」Westlaw Japan コラム特報第 10 号 2 頁

48) 保険に関する裁判例の中には故意との近似性という枠組みで重過失を捉えるのを積極的に否定する大阪高判昭和 55・9・24 判タ 440 号 146 頁もある。

また、②僅かであるが故意・重過失か否かを責任制限特約の有効・無効の分岐点としない裁判例があること、③重過失を著しい注意義務違反と捉える裁判例も基本的義務を措定してその初歩的な違反と捉えるもの、逸脱するパターンが過大なものなど、複数のパターンに分かれる<sup>49)</sup>。

### 3 本判決の重過失の認定

本件基本契約の責任制限特約が適用されるか否かは Y に重過失があるか否かにより決まることは本件でも同様であるが、本判決は次のようにして重過失を認定した。

まず、第 1 に、重過失を判断する注意義務の基準について、本判決は、Y が専門業者であることが注意義務の程度を基礎づける要素となることを判示し、Y の注意義務として高度な注意義務を措定した。

ベンダーはシステム開発の専門業者であり、ユーザーはシステム開発の専門家の知見を全面的に信頼して契約を締結することが一般的である。したがって、ベンダーに要請される注意義務の程度は、その専門的知見を背景に通常の場合よりも、高度な義務が認定されることは様々な裁判例からも明らかである。本件でも、X は、Y のシステム開発の専門業者であることを信頼して、本件システムの設計、保守等の委託契約を締結システム開発を発注しており、Y には専門家としての高度な注意義務が課されることは正当と思われる。

Y に高度な注意義務が課されることを前提として、第 2 に、注意義務違反の有無を判断する事情として、本判決は、① Y がプログラムに関する専門的知見を活用した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、X も Y 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ること、② SQL インジェクション対策がされていなければ、第三者が SQL インジェク

---

49) 遠藤元一「故意・重過失の法的責任と損害賠償（下）」市民と法 No. 86・25 頁

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流出する事態が生じ得ることをYは予見が可能であり、かつ、③経産省及びIPAが、QLインジェクション攻撃をウェブアプリケーションに対する代表的な攻撃手法であり、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、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、④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こと、⑤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して、重過失を認定した。

①②③は、結果の予見が可能であり、かつ容易であること、④⑤は結果の回避が可能であり、かつ（多大な労力が費用がかからないという意味で）容易であると評価する事情であり、「著しい注意義務違反（重過失）」というためには、結果の予見が可能であり、かつ容易であること、結果の回避が可能であり、かつ容易であることが要件となる」という誤発注控訴審判決の重過失の判断枠組みを踏襲していると捉えることができる。

誤発注控訴審判決は、不具合のあるシステム利用に関連して生起する損害を、軽過失＝免責、重過失≠免責というフィルターを通じて、いかに当事者間に適正に損失分担させるかという調整作業と捉えることができ、その調整作業として、発生した損失をどちらか一方当事者に完全に転嫁するのではなく、発注者の過失（株数と価格を逆にした明らかに異常な注文、東証からの確認の電話に対する対応の遅れ）と取引所の過失（不具合のあるシステムの提供と、誤発注か否かの確認と取消注文待ちをした対応の遅れ）<sup>50)</sup>とが競合して発生した損失を重過失の判断及び過失相殺概念を媒介して適正に分配する作業が行われている<sup>51)</sup>。

---

50) 小塚莊一郎「判批」ジュリ1436号113頁、河村賢治「判批」ジュリ1440号114頁

51) 遠藤・前掲注49) 25頁



本判決の事案は、システムの不具合から生じた損失をシステム開発契約を締結した当事者間で損失分担を扱うものであり、システム開発契約を締結した当事者間ではないシステム提供者とシステム利用者との間の損失分担を扱う誤発注控訴審判決とは事案を異にする。しかし、システム開発ベンダーの過失（システム開発に係わる債務不履行ないし瑕疵担保）とユーザーの過失（セキュリティ上は顧客のクレジットカード情報を保有しない方が良いことを認識し、Y から本件システム改修の提案をうけていながら放置）とが競合して発生した損失を重過失の判断及び過失相殺概念を媒介して適正に分配する作業を行っているという点では、本判決が重過失の判断につき誤発注控訴審判決と同様の判断枠組みを採用したことは自然であったといえる。

この重過失の判断枠組みが今後、どのような類型の事案にまで適用されうるのか、事例の集積を注視していく必要がある。