SLN SOFTIC LAW NEWS

一般財団法人ソフトウェア情報センター
発行・編集　　専務理事　光主清範

No. 142(2015/5)

東京地裁平成 26 年 1 月 23 日判決（東京地裁平成 23 年（ワ）第 32060 号）～ウェブサイトによる商品受注システムを利用した顧客のクレジットカード情報の流出事故につき、システムの設計、試作、保守等の受託会社の債務不履行に基づく損害賠償責任が肯定された事例～

弁護士　曽根 翼

1　はじめに

(1)　本件は、ウェブサイト上のオンラインショップを利用した顧客のクレジットカード情報が流出した事案について、受注システムの設計、製作、保守等を受託した被告に、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があることが認定され、委託者である原告が支出した顧客に係る謝罪・問い合わせ等の対応費用、流出判明後のシステム仮移行費用、事故対策会議の出席費用、売上損失等、様々な費目について債務不履行に基づく損害賠償請求が認容された事案である。

(2)　昨今、インターネットを介した個人情報の流出事案が多発しているため、個人情報を取り扱うシステム開発受託業者に要求されるセキュリティ対策の程度、情報流出の原因が明確に特定できない場合に要求される相当因果関係立証の程度、システム開発委託者に過失が認められる場合と過失の割合、損害賠償の責任限定合意の効力、流出事故と相当因果関係が認められる損害の範囲等について、事例的な意義を有する判決として紹介する。

2　事実関係の流れ

原告はインテリア商材の卸小売、通信販売等を行う株式会社である。被告は情報処理システムの企画、保守受託、顧客へのサポート業務、ホームページの制作、業務システムの開発、ネットショップの運営等を行う株式会社である。本件の前提事実及び裁判所が認定した事実関係の流れは、次のとおりである。

平成 21 年 1 月 30 日　原告と被告会社が業務委託基本契約等（以下「本件基本契約」という。）を締結した。

平成 21 年 2 月 4 日　原告が被告に、原告のオンラインショップサイト（以下「本件ウェ

〒105-0001 東京都港区虎ノ門 5-1-4 東都ビル 4 階
TEL. (03)3437-3071　FAX. (03)3437-3398
WebSite　http://www.softic.or.jp/

	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。）を 8,895,600 円（消費税込み。以下同じ。）で発注した。
平成 21 年 4 月頃	被告は原告用にカスタマイズしたウェブアプリケーション（以下「本件アプリケーション」という。）を製作して本件システムを完成させ、原告による検収を受けた。なお、被告は、S 社との間でサーバー利用契約を締結し、同社設置に係るレンタルサーバー（以下「本件サーバー」という。）に本件システムのデータを保存していた。
平成 21 年 4 月 15 日	本件ウェブサイトの稼働開始。この時点では、顧客はカード情報をクレジットカード会社が管理するウェブサイト画面上で入力するため、本件サーバー内のデータベース（以下「本件データベース」という。）に顧客のカード情報は送信されていなかった。
平成 21 月 4 月末頃	原告は被告に本件システムの利用（保守サービス及びサーバー利用）に係る初年度利用料（平成 21 年 4 月分～平成 24 年 1 月分）として合計 577,500 円（消費税込）を支払った（消費税別で月額 55,000 円であり、うち 25,000 円がサーバー利用料，うち 30,000 円が被告の標準保守サービス料（サーバー稼働確認，サーバー監視，サーバー障害対応及び原告からの問合せに対する対応業務）であった）。その後、本件システムの利用は一年ずつ更新され、最終更新では、本件システムの利用期間が平成 23 年 2 月～平成 24 年 1 月までとされた。
平成 22 年 1 月 26 日	原告は、本件ウェブサイトで顧客が利用した決済方法（金種）について、クレジットカード決済、代金引換、銀行振込みの区別しか把握できていなかったため、被告に、各種クレジットカードの種別（カード会社名）を原告の基幹システムに送信する旨の仕様変更（以下「金種指定詳細化」という。）を代金 315,000 円で発注した。
平成 22 年 1 月 29 日	被告は、この日までに金種指定詳細化を導入した本件システムについて原告による検収を受け、同日に導入後のシステムを稼働させた。同日以降、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と、本件サーバーに顧客のカード情報が入力され、その後、本件サーバーとカード会社との間でカード情報のやり取りが行われるようになり、カード情報は暗号化されずに本件データベースに保存されるようになった。なお、被告は、金種指定詳細化を導入するにあたり、クレジットカード番号の先頭 6 桁のみでカード会社を識別できたが、本件サーバーにクレジットカード情報全部を保存する設定とし、そのうちカード会社名の情報のみを原告の基幹システムに送信する設定とした。また、被告は、各種クレジットカード種別を原告の基幹システムに送信する方法を提案したが、送信する情報の具体的な内容は原告が指定することとされたため、原告はカード会社名の情報のみを基幹システムに送信することを被告に要求した。そのため、原告はカード会社情報以外のクレジットカード情報を見ることはできなかった。

平成 22 年 5 月 1 日　原告と被告は、本件ウェブサイトのデザイン変更等を内容とするメンテナンス契約を締結した（それまでは変更依頼の度に料金が発生していた。）。

平成 22 年 9 月　被告取締役が原告担当者に、金種指定詳細化当時はカード会社を判別するためクレジットカード番号を取得する必要があったが、この時点ではカード会社のシステム上で決済をした後にカードが会社を判別することが可能となったため、金種指定詳細化以前と同様の方式でカード会社名を取得することができ、その仕様変更費用が 20 万円程度であること、「クレジット情報は保持しないのがセキュリティ上より良く、一般的です。」等の内容をメールで伝えたが、原告はその後も、本件データベース上のクレジットカード情報の削除、暗号化等を指示しなかった。なお、原告担当者は、メールのやり取りを通じて本件データベースにクレジットカード情報のデータがあるが，本件データベースを直接見る手法を用いなければ当該情報を見られないことを認識していた。

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外部に流出した（以下「本件流出」という。）。

3　本件システム等の構成

(1)　本件システムは、本件ウェブサイトに表示された商品を顧客が注文してクレジットカード決済するためのものであり、本件ウェブサイトと原告の売上げ及び在庫管理に関する基幹システムを連携させ、オンラインでの注文確定を可能とするものであった。被告は、無償配布ソフトウェアである EC-CUBE をカスタマイズした Web 受注システムを本件以前から販売しており、これを原告用にカスタマイズした本件アプリケーションを本件システムに用いていた。EC-CUBE はクレジットカード情報を扱う仕様だったが、原告がカスタマイズした受注システムはクレジットカード情報を扱う仕様を有していなかったため、被告は本件システムにクレジットカード情報を扱う機能を製作して実装した。なお、本件アプリケーションには、SQL インジェクション対策として独立行政法人情報処理推進機構（以下「IPA」という。）が推奨する SQL インジェクション対策であるバインド機構[1]の使用及びエスケープ処理[2]がいずれもなされていない部分があった。

(2)　本件システムのデータは、被告が S 社からレンタルした本件サーバー内の本件データベースに保存されていた。保存される情報は、金種指定詳細化前までは商品情報、氏名・住所等の顧客情報及び注文情報であったが、金種指定詳細化以降はクレジットカード情報

[1] バインド機構とは、予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である。

[2] エスケープ処理とは、SQL 文において特別な意味を持つ特殊文字（「', 「；等）を無効化する処理である。独立行政法人情報処理推進機構（IPA）発行に係る「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」においては、バインド機構を使用できない場合に、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が推奨されている。

（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）も保存されるようになった。本件では、本件サーバーに保存されるようになったこのクレジットカード情報が流出したことに関して、原告が被告に損害賠償請求をしたものである。

(3)本件データベースから原告の基幹システムに送信される情報は、金種指定詳細化前までは商品情報、顧客情報及び注文情報であったが、金種指定詳細化以降はさらにカード会社名も送信されることになった。

4　争点

本件の争点は、下記の争点①ないし⑤である。本件流出の原因に関する争点①では流出原因が 4 つ主張され、被告の債務不履行の有無に関する争点②では被告の債務不履行が 5 つ主張された。また、争点③においては因果関係の断絶の有無、争点④においては損害額、争点⑤においては損害賠償責任合意の成否等が問題となった。

(1)　争点①（本件流出の原因及び程度）

原告は、本件流出の原因は次のいずれかであり、合計 1 万 6798 件の顧客の個人情報（うちカード情報が含まれるものは 7316 件）が流出したと主張した。これに対し、被告は、本件流出が発生したこと自体は認めたが、個人情報の流出件数と流出の原因は不明であると主張して反論した。

①　SQL インジェクション

SQL（Structured Query Language）とは、データベースの管理プログラムを制御するためのコンピュータ言語である。SQL インジェクションは、本件判決では、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、プログラム作成者の予想していない SQL 文を実行させることであると定義されている[3]。

本件において、原告は、本件流出に関して、平成 23 年 4 月 19 日には顧客のクレジットカード情報の不正利用が確認されたところ、事後の調査により、平成 22 年 12 月 7 日から平成 23 年 4 月 14 日までに本件サーバーに対して外部から攻撃するための事前調査が行われたこと、同日午前 10 時 31 分から午前 10 時 36 分まで継続的に本件データベースに SQL インジェクション攻撃がされ、その際、窃取した内容がアクセスログに記載されない攻撃手法が用いられていたこと、上記攻撃による通信が成功したことを示すコードが表示されたこと及び本件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（バインド機構の使用及びエスケープ処理がされていないこと）が存在したことが判明しており、SQL インジェクション攻撃によって本件流出が発生したことが裏付けられていると主張した。

②　サーバーへのリモートログイン

データベースが保存されているサーバーにログインし、さらに当該データベースにログ

[3] 「平成 18 年 2 月 20 日付け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措置」においては、データベースの管理プログラムを制御するための特殊な文字言語である SQL を用いて、外部から直接データベースを操作して、データの改ざん、書き換え、情報の搾取等を行うことであると定義されている。SQL インジェクションや後述するクロスサイトスクリプティングは、いずれもプログラム開発時のコーディングミスによる脆弱性を突いた攻撃である。

インして、当該データベース内に保存されている情報を読み出す方法である。
本件において、原告は、外部からリモートログインＩＤ及びパスワードを入力して本件サーバーにリモートログインした上で、さらにデータベースログインＩＤ及びパスワードを入力して本件データベースにアクセスして顧客の個人情報を読み出すことができたと主張した。

③　管理機能への不正ログイン
インターネット上のウェブページのうち、通常は閲覧者が利用することを予定していない管理機能に管理者のログインＩＤ及びパスワードを用いてログインし、管理者としてアプリケーションを操作し、当該アプリケーションの動作を通じてデータベースに保存されている情報を読み出す方法である。
本件において、原告は、外部から、管理機能ログインＩＤ及びパスワードを入力して管理機能にログインし、本件ウェブアプリケーションを操作して本件データベースにアクセスして顧客の個人情報を読み出すことができたと主張した。

④　クロスサイトスクリプティング
クロスサイトスクリプティングとは、利用者によるウェブサイト閲覧時に出力されるウェブページに悪意あるスクリプト（簡易的なプログラム言語）を埋め込み、そのスクリプトを標的ウェブサイトに転送し、標的ウェブサイトがスクリプトを排除しない欠陥を介して、当該スクリプトをブラウザで実行する攻撃である。
本件において、原告は、クロスサイトスクリプティングによって、本件ウェブサイト上に偽のページが表示され、フィッシングサイトへ誘導し個人情報を入力させるなどして個人情報が流出したか、又は顧客のブラウザ上で不正なスクリプトが実行され、ブラウザが保存している Cookie 情報が漏洩し、Cookie 情報に含まれている個人情報が流出した可能性があると主張した。

(2)　争点②（被告の債務不履行責任の有無）
原告は、被告との間で締結した本件基本契約、同契約に基づく個別契約、本件ウェブサイトのメンテナンス契約をそれぞれ締結しているところ、本件システムの開発及び導入がなければ原告が被告に対して本件システムの変更及び保守や金種指定詳細化を委託することもなかったこと、各個別契約は密接不可分な関係性を有すること、当事者間の意思としても各個別契約を一体として捉えるのが合理的であることからすれば、これらは一体の契約としてみるべきであり、被告はこの一体の契約に基づき、下記①ないし⑤の債務を負担し、これらの債務不履行責任を負うと主張した。

①　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)

②　債務不履行 2（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）

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

④　債務不履行 4（サーバー、データベース及び管理機能へのログインＩＤ及びパスワードを管理すべき債務の不履行）

⑤　債務不履行 5（被告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）

原告は、本件流出の原因が SQL インジェンクションである場合には債務不履行 1、3、5 を、サーバーへのリモートログイン又は管理機能への不正ログインである場合には 1 ないし 5 の責任を、クロスサイトスクリプティングによる場合には債務不履行 1 の責任を負うと主張した。

(3)　争点③（原告の過失と因果関係の断絶）

被告は、本件流出の直接的原因は、原告が被告に金種指定詳細化のために本件データベースに顧客のカード情報が保存されるように仕様変更することを被告に委託したためであり、その後、その安全性及び改善の方法等に関して原告が被告に質問をした際に、原告は被告から具体的な費用と共に改善の方法等を指摘されたにもかかわらず、当該仕様を放置したのであり、原告は、このような過失により自ら本件流出を招いたものと評価すべきであるから、被告の債務不履行と本件流出との間の因果関係は、原告の行為によって断絶されたと主張した。

(4)　争点④（損害）

原告は、被告の債務不履行により被った損害として、ウェブ受注システム委託契約に関連して支払った代金、顧客への謝罪関係費用（QUO カード及び包装代、郵送代等）、顧客からの問合わせ対応のためのコールセンター費用、本件流出原因の調査委託費用、本件流出が発生したことによる外部データセンターの使用料、事故対策会議出席交通費、売上損失等として、合計 109,584,809 円の損害を請求した。

(5)　争点⑤（損害賠償責任の合意の成否等）

本件基本契約書には、下記の規定が存在したが、契約書の規定が内容ごとに章立てされていることもあり、これらの条項の解釈について争いとなった。

（本件基本契約書　抜粋）

第 7 章　機密保持

第 25 条〔損害金〕

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。

第 8 章　保証及び管理

第 26 条〔保証〕

乙は，委託業務の完了の後その成果物に瑕疵が発見されたとき，乙の責任において無償で速やかに補修のうえ納入を行うものとする。（1 項）

乙の保証期間は，特に定めるものを除き委託業務の完了の後 1 年間とする。ただし，乙の責に帰すべきものでない場合はこの限りではない。（2 項）

第 9 章　損害賠償その他

第 29 条〔損害賠償〕

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。（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）

ア　被告は、本件基本契約 25 条は民法の原則どおり損害賠償義務を負うことを確認したものであり、同契約 29 条 2 項は被告の損害賠償額を制限したものであると主張した。また、同項は被告に重過失がある場合に適用が排除される旨は規定されていないため、被告に重過失があっても適用されると主張した。

イ　これに対し、原告は、本件基本契約 29 条 2 項が同契約 25 条の特則である旨は明記されておらず、同条が本件基本契約の第 7 章「機密保持」の規定に違反した場合の損害賠償の特則と解すべき根拠はないから（特則と解すると機密の保持の場合のみ全額賠償となる。）、当事者の合理的意思としては、相当因果関係がある損害全額の賠償を合意したものであり、損害賠償額を制限する旨の合意は成立していないと主張した。また、原告は、損害賠償額を制限する特約が契約内容となるためには、民法の一般原則を排斥する両当事者の明確な個別的合意が必要であるところ、本件基本契約 29 条 2 項が同契約 25 条に優先適用される旨の説明を被告が原告にしていないこと、本件委託契約書は専門業者である被告が作成したものであり、経済産業省が作成したモデル契約書と内容が異なることから、損害賠償額制限について個別的な合意は成立していない等と主張した。

5　争点に対する裁判所の判断

(1)　争点①（本件流出の原因及び程度）

①　本件流出の原因

裁判所は、本件データベースに顧客のカード情報が暗号化されずに保存される設定となっていたこと、信販会社二社が平成 23 年 4 月 20 日に原告からクレジットカード情報が流出した疑いがあると警告を行ったことから、同日までに流出が発生したと認定した。

原告は、本件流出が発生してすぐにセキュリティソリューションサービス事業者である株式会社ラック（以下「ラック報告書」という。）と verizon business 社（以下「ベライゾン報告書」という。）に本件流出の原因及び被害範囲の特定について調査を依頼して 2 通の調査報告書を作成し、これらを証拠として提出している。ラック報告書は、流出の原因について、ログ調査の結果、平成 22 年 12 月 7 日から平成 23 年 4 月 14 日まで SQL インジェクション攻撃による断続的な事前調査が行われ、同日午前 10 時 31 分から同 36 分までの 5 分間に海外ＩＰアドレスから 1508 回に及ぶ POST メソッドによる SQL インジェクション攻撃（窃取内容がアクセスログに記録されない方法）が行われたと確認でき、同日のログでは外部との通信が成功したことを示すコードが表示されていたこと、また本件アプリケーションには SQL インジェクション攻撃に対する脆弱性が存在することから、本件流出の原因は SQL インジェクションであると推測できるとした。原告が主張するその他の流出原因についてもその可能性を指摘した。これに対し、ベライゾン報告書では、データ漏洩に関する決定的な証拠はなく、攻撃者が SQL インジェクションを実行したことは確認したが、攻撃者がクレジットカード保有者データベースにアクセスした証拠はなく、原告が主張するその他の流出原因についても、そのうちクロスサイトスクリプティングについてのみ攻撃が試みられたことが確認されたとしたが、悪意のあるソフトウェアが実際にダウンロードした証拠はないとした。

裁判所は、株式会社ラックは国内最大規模でネットワーク・セキュリティー監視業務を行っており、ネットワーク・セキュリティーについて専門的知見を有すると認められること、プログラムの一か所でも脆弱性があるとその部分に SQL インジェクションを繰り返すことにより個人情報を窃取することが可能であること、本件アプリケーションにはバインド機構の使用及びエスケープ処理がいずれもなされていない部分があること等から、ラック報告書は専門的知見にも合致するものであり信用することができるとし、ベライゾン報告書も SQL インジェクション攻撃の痕跡を指摘するものであるため、ラック報告書と矛盾するものではないとした。

また、本件は訴訟継続中に民事調停手続きに付されており（民事調停法 20 条 1 項）、プログラムの専門家が調停委員に加わっている。調停委員会は、流出した情報の内容及び流出時期が不明であり情報の内容及び流出日時から本件流出の原因を特定することができないこと、カード会社による情報流出に関する警告がどのような根拠及び判断に基づいて行われているか不明であり顧客がクレジットカード決済を行った他のウェブサイトが流出原因である可能性も否定しきれないこと、流出原因に関する直接証拠がないことから、SQL インジェクションが本件流出の原因であるとの立証は尽くされていない旨の意見書を作成している。

しかし、裁判所は、本件流出が発生したことは事実であること、同報告書においても個人情報を不正取得するための手段として最も可能性が高いのは SQL インジェクションであると指摘されていること等から、本件流出の原因は平成 24 年 4 月 14 日の SQL インジェクションであると認定した。なお、原告が主張するその他の流出原因についてはいずれもこれを裏付ける証拠がないとして認めなかった。

② 流出の程度

裁判所は、流出件数について、漏洩した情報の内容と件数は正確には不明であるとしつつ、「最大で」クレジットカード情報 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あると認定した。これらは両報告書記載流出件数のうち多いほうの件数（クレジットカード情報についてはベライゾン報告書、クレジットカード情報を含まない個人情報についてはラック報告書）を「最大で」との留保付きで採用したものである。判決では「少なくとも」というような控えめな認定をすることが多いため、比較的珍しい認定であると思われる。

(2) 争点②（被告の債務不履行責任の有無）

裁判所は、原告が被告との間で締結した本件基本契約、同契約に基づく個別契約、本件ウェブサイトのメンテナンス契約を一体の契約としてみるべきであると主張した点については、これらが別な時期に締結されたものであり、個別契約ごとに内容も異なることから、一体の契約としてみることはできないと判断した。

その上で、本件流出の原因が SQL インジェクションであることを前提として、その場合に流出の原因であるか否かが問題となる債務不履行 1、3、5 についてのみ検討した（債務不履行 2、4 は、流出の原因がサーバーへのリモートログイン又は管理機能への不正ログインである場合のみ問題となるが、上述のとおり、流出の原因は SQL インジェクションであると認定されたため、これらは争点として判断されなかった。）。

① 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）

債務不履行 1 の成否を検討する前提として、被告が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について本件各契約に明文の規定がないため、そもそも原告が当該債務を負っていたかが問題になる。

この点について、裁判所は、被告が本件システムの発注を受けたことをもって、「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」と認定し、さらに本件システムでは、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」と判断した。

そして、裁判所は、当該債務の不履行があったか否かについて、(i)経済産業省が平成 18 年 2 月 20 日に「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、(ⅱ)IPA は、平成 19 年 4 月に「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ることからすると[4]、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うことができるが、本件アプリケーションには、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ったことから、被告は債務不履行 1 の責任を負うと認定した。

② 債務不履行 3（カード情報を保存せず、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 も同様に、その成否を検討する前提として、被告が金種指定詳細化の業務契約を締結した際に、クレジットカード情報を保存せず、保存する場合には暗号化すべき債務を負っていたかが問題となる。

この点についても、裁判所は、公的機関等が公表していた文書を重要した判断をしており、(ⅰ)厚生労働省及び経済産業省が平成 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」（同日厚生労働省・経済産業省告示第 1 号）においては、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要最小限の保存期間を設定すること、保存場所を限定すること、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ていたこと、(ⅱ)IPA が同年 4 月に前記「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」と題する文書において、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を暗号化することが望ましいと明示していたことを指摘している。しかし、裁判所は、争点 1 の場合と異なり、これらのガイドライン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ものであり、また上記 IPA の文書では、データベース内のデータ全てに暗号化処理を行うとサーバーの負荷になることがあるので、特定のカラムだけを暗号化するなどの考慮が必要であるとも指摘されていたことから、暗号化の設定内容等は暗号化の程度によって異なり、それにより被告の作業量や代金も増減すると考えられるため、契約で特別に合意していなくとも当然に被告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、若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ず、被告に債務不履行 3 の責任を負わないと判断した。

③ 債務不履行 5（（被告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）

原告は、システム設計、開発及び運用を行う業者である被告が原告に対し、本件システムのセキュリティ対策の程度及び情報流出の危険性を認識し、セキュリティ対策について選択できるように説明すべき信義則上の義務を負っていたものであり、その説明すべき具体的内容は、(ⅰ)SQL インジェクション対策を講じていないこと、(ⅱ)本件システムのセ

4 IPA の「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」においては、「SQL インジェクションによる攻撃を防ぐためには、プログラミングの時点から不正な SQL 文を実行しないように対策することが必要である。以下に、SQL インジェクションの対策方法を示す。」「・SQL 文の組み立てにバインド機構 を使用する。バインド機構を使用できない場合は、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」とされている。

キュリティ対策が脆弱であること、(ⅲ)被告とA株式会社との間のレンタルサーバー契約において最低のセキュリティレベルの内容としていたこと、(ⅳ)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としたことであったと主張した。

裁判所は、(ⅰ)について、被告は上述のとおり、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契約上の義務を負うのであるから、それとは別にSQLインジェクション対策を講じていないことを説明すべき信義則上の義務を負うとは認められないとした。(ⅱ)については、本件流出の原因はSQLインジェクションと認められる一方で、その他のセキュリティ対策が脆弱であることが本件流出に寄与したことを認めるに足りる証拠がないこと、(ⅲ)についても、レンタルサーバー契約において最低のセキュリティレベルとしていた証拠がないことから、いずれについても被告が説明義務を負うとは認められないとした。最後に、(ⅳ)についても、原告のシステム担当者は、被告の取締役からの回答により、データベースにクレジットカード情報のデータはあるがデータベースを直接見る手法を用いなければカード番号は見られないこと、セキュリティ上はクレジットカード情報を保持しない方が良くその方が一般的であるとの説明を受けていたことから、被告に説明義務違反は認められず、結論として、被告は債務不履行5の責任は負わないと判断した。

(3)　争点③（原告の過失と因果関係の断絶）

裁判所は、被告が金種指定詳細化をするに当たり、本件データベースにクレジットカード情報を保存する必要性があったとは認められず、仮に保存するとしてもカード会社を識別することのできる先頭6桁の番号のみで足りたのに、被告はクレジットカード情報を保存することを選択したのであるから、原告が金種指定詳細化を依頼したことにより被告の債務不履行1と本件流出との因果関係が断絶すると解することはできないとした。

また、原告が被告から本件システムの改修提案等を受けていたにもかかわらず、原告が本件データベースにクレジットカード情報が保存される使用を放置したとの点についても、裁判所は、本件流出はSQLインジェクション対策を怠るという被告の債務不履行1による危険が現実化したものであり、原告が改修を実行しなかったことは本件流出という結果を招来したものではないから被告の債務不履行1と本件流出の条件関係を否定するものではなく、因果関係が断絶すると解することはできないとした。

なお、当事者から過失相殺の主張はなされなかったが、裁判所は、被告から本件システムの改修提案を受けていながら原告が何ら対策を講じずに放置したことを原告の過失として考慮し、3割の過失相殺をすることが相当であると職権により判断した。

(4)　争点④（損害）

裁判所は、原告が主張する損害のうち、次のものを被告の債務不履行と相当因果関係のある損害として認めた。損害額は合計3231万9568円であるが、上記の過失相殺3割を考慮して減額されたため、実際の認容額は2262万3697円となった。

(1)　本託契約に関連して支払った代金　27万5625円

原告は、被告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得なくなったとして、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合計2074万1175円を請求したが、裁判所は、原告が別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日までは、被告との契約に基づき提供され

たサービスによる利益を享受していたのであるから、被告に債務不履行があったとしても、本件個別契約に基づき支払った代金全額が当然に損害となるものではないとして、原告の主張を認めなかった。しかし、裁判所は、原告は、平成 23 年 9 月以降については被告による保守サービスを受けず本件サーバーも利用していなかったため、同月以降分として支払済みの保守サービス料及びサーバー利用料を損害として認めた。

(2)　顧客への謝罪関係費用　1863 万 7440 円

裁判所は、原告が負担した顧客への謝罪関係費用のうち、下記合計 1863 万 7440 円を損害として認めた。

ア　QUO カード及び包装代　1636 万 2342 円
イ　お詫びの郵送代　124 万 6459 円
ウ　お詫び郵送に係る資材費及び作業費　86 万 7196 円
エ　告知郵送代　8 万 1440 円）
オ　告知の封筒代　1 万 0500 円）
カ　お詫びのメール配信の外注費　6 万 6843 円
キ　お詫び及び QUO カードの書留郵便代　2660 円

(3)　顧客からの問合せ等の対応費用　493 万 8403 円

(4)　調査費用　393 万 7500 円

原告は、本件流出に関する上記調査報告書作成費用として、合計 393 万 7500 円を支払ったため、これを損害として被告に請求した。裁判所は、本件の調査には専門的な知見が必要であること、早急に調査を行う必要があったこと、上記二社の作成した報告書は内容が異なるように各自がその専門的な知見を活かして作成されたものであることからすれば、原告が二社に調査依頼をしたことは相当性を欠くといえないとして、二社に対する調査費用全額を損害として認めた。

(5)　ラックのデータセンター使用料　42 万円

原告は、本件流出発生後の平成 23 年 4 月 30 日から別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同年 8 月 23 日までの 4 か月間において、データセンター利用料（サーバー利用料）として 42 万円を支出したが、裁判所はこれを全額損害として認めた。

(6)　事故対策会議出席交通費　4 万 7600 円

(7)　転職や求人情報に関するウェブサイトの応募フォーム変更　6 万 3000 円

原告は、サーバーを変更したことにより転職や求人情報に関するウェブサイトである応募フォームを変更する必要が生じたため、別会社に変更を依頼した費用として 6 万 3000 円を支出しており、裁判所はその全額を損害として認めた。

(8)　売上損失　400 万円

原告は、本件流出により平成 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り、この期間にインター

ネット上で商品を販売できていれば、少なくとも 6041 万 4833 円を売り上げることができたと主張して同額を損害賠償として請求した。しかし、裁判所は、原告に一定の売上減少があったことは推認することができるとしたものの、原告から具体的な売上減少額を明らかにする決算書類等は提出されておらず、売上金額から控除すべき仕入原価等を立証することは困難であるとして、4,000,000 円の限度で被告の債務不履行と相当因果関係のある損害と認めた（民訴法 248 条）。

(5)　争点⑤（損害賠償責任の合意の成否等）

①　損害賠償額制限の合意の成否

裁判所は、本件基本契約書の構成（章立て）に忠実に解釈し、本件基本契約書の「第 9 章　損害賠償その他」に規定されている 29 条 2 項は、被告の原告に対する損害賠償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ものであり、同契約書「第 7 章　機密保持」に規定されている 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とし、同内容の契約が成立したことを否定すべき特段の事情も存在しないと判断した。

②　本件基本契約 29 条 2 項の適用の有無

裁判所は、本件基本契約 29 条 2 項の趣旨について「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」が、「被告（省略）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。）。」と判示し、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判断した。

本件においては、原告は被告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ものであり、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、SQL インジェクション対策がされていなければ第三者からの攻撃により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 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り、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から、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として、裁判所は被告に重過失が認められると判断した。

6　検討

(1)　判決では、争点②（被告の債務不履行責任の有無）の判断にあたり、受託者である被告に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（債務不履行1）を認定するにあたり、経済産業省及びIPAの発行に係るセキュリティ対策に関する文書において、SQLインジェクション対策を採ることが必要である旨が記載されていたことを重視している。

これに対し、カード情報を保存せず、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）の判断にあたっては、厚生労働省及び経済産業省の個人情報保護に関するガイドライン並びにIPAの上記文書において、当該措置を採ることが望ましいものと記載されているにすぎず、必要であると記載されていなかったことを重視し、かかる債務を被告が負担しないものと判断している。

これらの債務は、いずれも原告と被告との間で交わされた契約書に直接記載されていない点及び受託者である被告がこれらの債務を履行する場合には、そうでない場合と比べてより多額のコストが発生することになる点において共通する。しかし、判決においては、信用性のあるセキュリティ対策に関する文書や該当分野における個人情報に関するガイドラインの記載を重視し、被告の債務負担の有無について両債務で結論を異にしたものであり、この種の事案において裁判所がいかなる証拠資料を重視するかにつき、参考になるといえる。

(2)　また、争点⑤（損害賠償責任の合意の成否等）において、当事者からは、損害賠償額制限の合意の成否とその適用範囲等に関する本件基本契約書の解釈について、様々な主張がなされたが、判決においては、損害賠償額を制限しないと規定する25条が「第7章　機密保持」に関する章に規定されていることを重視し、損害賠償額が原則として制限されないのは機密保持義務違反の場合のみであり、その他の損害賠償額については、「第9章　損害賠償その他」に規定されている損害賠償額の制限条項である29条2項が原則として適用される旨判断されている。

本件基本契約書を素直に解釈すれば、特段の事情がない限り、裁判所のような判断に至るものと思われるが、実務上、契約書を作成する際には、個々の規定はもとより、全体の構成（章立て）についてもよく検討し、このような疑義が生じないような規定振りとすべきであろう。

(3)　また、本件基本契約書29条は、その1項において「乙又は乙の技術者の故意又は過失により」損害を与えた場合に被告が損害賠償責任を負う旨を規定し、同条2項では、その場合の損害賠償額を個別契約の契約金額を上限とする旨を規定している。このように、本件基本契約書には、被告が重過失により損害を与えた場合における損害賠償責任の発生の有無は明記されていないが、同条1項により被告は軽過失の場合に損害賠償責任を負うのであるから、重過失の場合にはなおさら責任を負うべきことは当然である。しかし、判決においては、被告に重過失がある場合に損害賠償額が制限されるのは、著しく衡平を害するものであり、当事者の通常の意思に合致しないとの理由により、同条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判示している。確かに、事業者同士の契約であっ

ても、専門的な分野に関するものであり、当事者に情報や能力の格差があるときには、衡平性や当事者の通常の意思を重視すべき場合があることは勿論であり、本件の結論としては妥当であると思われる。

しかし、故意に損害を与えた場合はともかく、契約書における損害賠償額の制限条項において、重過失にあたる場合が排除されていないにもかかわらず、衡平性や当事者の通常の意思を重視して規定と異なる解釈をすることは、軽過失と重過失の線引きが必ずしも容易でないことも考慮すると、妥当な結論を導くことがある一方で、契約当事者から契約の予測可能性を奪うことにもつながりかねない。

本件では、本件基本契約書に被告に重過失がある場合について、何ら記載が存在しないが、実務上は、紛争を予防するために、重過失が認められる場合に当該規定が適用されるか否かについて、そのような規定にする経緯や理由も含めて契約書に明記しておくべきであろう。このようにすれば、紛争に至った場合においても、衡平性や当事者の通常の意思を根拠として契約書の規定と異なる解釈がなされることを一定程度は予防でき、契約の予測可能性を確保できると思われる。民法（債権法）の改正条文においても、従来よりも当事者の合意内容が重視される内容が盛り込まれていることからすると、今後はより当事者の具体的意思を重視する契約書の解釈がなされる可能性がある。その対応策としての意味でも、日本国内の当事者同士で締結される契約書においても、英文契約書に見られるような充実した前文条項や目的条項（Whereas Clause）を盛り込むことが有用であろう。

以上