東京地裁平成26年1月23日判決
＜東京地判平成23年（ワ）第32060号＞

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おいて、システム開発を受託した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案

発表者
小林　毅郎（大日本印刷株式会社）
武田　勝弘（スクワイヤ外国法共同事業法律事務所）

1. 事案の概要

- 原告は、インテリア商材の卸小売及び通信販売等を事業とする会社。
- 被告は、情報処理システムの企画・保守受託及び業務システムの開発等を事業とする会社。
- 原告は、被告との間で委託契約を締結し、ウェブサイトにおける商品受注システムの設計や製作等を被告に発注し、納品後、業務において使用を開始。
- 使用開始後、原告の顧客のクレジットカード情報の不正利用が確認されたため、調査等を行った結果、外部からの不正アクセスにより、原告のサーバーよりクレジットカード情報を含む個人情報の流出が疑われた。
- 上記より、原告は、顧客等への謝罪・対応や売り上げの減少等が発生したため、被告に対して、委託契約における債務不履行があったとして損害賠償を請求。

2. 訴訟までの経緯

- **平成21年1月30日**：原告と被告は、業務委託基本契約書及び被告による保守等の業務遂行が不可能となった場合の対処方法に関する覚書を締結。
- **平成21年2月4日**：原告は、注文書にて、ウェブサイトにおける商品のウェブ受注システムを被告に発注。
- **平成21年4月頃**：被告は、カスタマイズしたアプリケーションを製作すると共に、システムを完成させ、原告による検収を受けた。
- **平成21年4月15日**：原告は、ウェブサイトの稼働を開始。（※この時点では、サーバー内のデータベースに顧客のクレジットカード情報が送信される仕組みにはなっていない。）
- **平成21年4月末頃**：原告は、被告にシステムの初年度利用料を支払う。（※その後、1年ずつ更新し、最後の更新にて利用期間を平成24年1月までとした。）

2. 訴訟までの経緯

- **平成22年1月頃**：原告は、ウェブサイトにおいて顧客が利用した決済方法（金種）について、現状把握可能な、クレジットカード決済又は代金引換若しくは銀行振込の区別に関する情報以外に、自己の基幹システムに各種クレジットカード種別を送信する旨の仕様変更を被告に対し依頼し、**同月26日**に注文書を交付した。
- **平成22年1月29日**：被告は、上記の機能を導入したシステムの原告による検収を受け、稼働を開始。
- **平成22年5月1日**：原告と被告は、Webサイトメンテナンス契約書を締結する。
- **平成23年4月**：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した疑いが生じる。

3. 事実関係

1）原告と被告の間で締結された契約の概要

- 個別契約の代金の合計額は、1975万3500円（消費税込で、2074万1175円）。
- 原告は、ウェブサイトが稼働した平成21年4月分から平成24年1月分まで、システム利用料として月額5万5000円を支払い、うち2万5000円がサーバー利用料で3万円が標準保守サービス料である。
- 被告の標準保守サービスは、サーバー稼働確認、サーバー監視、サーバー障害対応及び問い合わせに対する対応業務である。

3. 事実関係

2)システム等の概要

- ウェブサイトに表示された商品を顧客が注文及びクレジットカード決済することを可能とし、原告の売り上げ及び在庫管理に関する基幹システムとウェブサイトを連携させ、オンラインでの注文確定を可能とするシステム。
- 被告は、電子商取引用ウェブサイトシステム構築のための無償配布ソフトウェアであるEC-CUBEをカスタマイズし、Web受注システムソフトウェア「△△△」を販売している。なお、本件では、「△△△」を原告向けにカスタマイズしたアプリケーションである。
- EC-CUBEは、クレジットカード情報を扱う仕様であったが、△△△はクレジットカード情報を扱う仕様となっていなかったため、クレジットカード情報を扱う機能を製作してアプリケーションに実装している。
- データベースファイルは、サーバー内(データベース)に保存されている。保存される情報の内容は、**金種指定詳細化の前までは、**商品情報、顧客情報(氏名、住所、電話番号、メールアドレス、パスワード等)及び注文情報であり、**金種指定詳細化以降は、**更に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。以下同じ。)が追加された。

3. 事実関係

3）金種指定詳細化に関する経緯

- 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、当該**基幹システムに送信される情報の具体的内容は、原告が指定**することとされた。
- 原告は、クレジットカード情報のうち、**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ことを要求**した。
- 被告は、金種指定詳細化を導入するに際して、顧客がウェブサイトでクレジットカード決済を行う場合、サーバーにクレジットカード情報が入力され、**クレジットカード情報のうち、カード会社名の情報だけを原告の基幹システムに送信する設定とした**。
- 被告は、上記に加え、クレジットカード番号の**最初の6桁の番号だけでカード会社を識別することが可能**だが、**データベースにクレジットカード情報全部が保存される設定**とした。
- 原告のシステム担当者は、**顧客のクレジットカード番号等を見ることが可能な設定であることを認識していた**ことに加え、**被告から“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、一般的である”との回答を受けた**にもかかわらず、データベース上のクレジットカード情報の**削除や暗号化等を指示しなかった**。

3. 事実関係

4）流出が発覚した経緯

- F株式会社（他のクレジットカード会社から、Xからクレジットカード情報が漏洩している可能性がある旨の連絡を受けて、調査した結果）からの問い合わせ、及び株式会社Gの警告（不正利用された者が共通に利用している店舗が原告のウェブサイトであったため）により発覚。
- 不正利用（不正利用の可能性があるため未決済も含む）の件数は、平成23年4月の1日から11日までは0件であったが、それ以降、以下のように件数が増えた。

  12日：1件 → 14日：3件 → 15日：4件 → 18日：2件

  → 19日：10件 → 20日：5件

（※その後も複数件の不正利用が発生）

4. 判決の内容

＜争点①：流出の原因及び程度＞

裁判所の判断：

流出の原因は、以下の理由に基づき、SQLインジェクションであると認められるとし、また、流出の程度は、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あるとした。

（1）**第三者の報告書から**、ウェブアプリケーションが**SQLインジェクションに対して脆弱であることが認められる**こと。

（2）ログ調査の結果、平成23年4月14日午前10時31分から5分間の間に海外IPアドレスから1508回に及ぶ**SQLインジェクション攻撃がされ、同日に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る**。

（3）過去に原告で利用されたことがあるクレジットカード情報が不正利用された件数が、平成23年4月14日から同月20日の間で、2件ないし10件と増加していること。

4. 判決の内容

＜争点①：流出の原因及び程度＞

(4) ウェブサイトにおいて**1か所でも予想しないSQL文の実行が可能な状態にあれば、**想定しないSQL文の実行を繰り返し、クレジットカード情報等の個人情報が格納された場所を探した後、その場所からSQL文を実行し、**全ての情報を窃取することが可能であることが認められる**。

(5) 不正利用が発生した複数会員における過去共通の利用店舗として原告が該当したことから警告がなされ、原告以外の店舗には警告していないことが認められることから、**Fが原告をクレジットカード情報の漏洩元と判断したことは合理的な理由が存在する**。

(6) **原告以外の第三者がFの会員のクレジットカード情報の漏洩元であることをうかがわせる事実もなく、Gも同月20日頃に原告がクレジットカード情報の漏洩元と判断していること**。

4. 判決の内容

＜争点②：被告の債務不履行責任の有無＞

裁判所の判断：

原告の請求のうち、当時の技術水準に基づき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の不履行のみ認定し、クレジットカード情報を保存せず、保存した場合であっても削除する設定や暗号化して保存すべき債務、及び被告の原告に対する説明する債務の不履行は認定しなかった。

4. 判決の内容

- 被告が必要となる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の不履行が認められるとした理由。

(1) **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**。

(2) **金種指定詳細化以前から、顧客の個人情報をデータベースに保存する設定となっていたため**、これら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るべきである。

(3) **経済産業省は、平成18年の時点で、**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おり**、被告は、契約締結時点で、エスケープ処理を施した、または、バインド機構を使用したプログラムを提供する債務を負っていたということができるが、いずれも行われていなかった部分が存在すること。

4. 判決の内容

- 被告が当然にクレジットカード情報を保存せず、保存した場合であっても削除する設定や暗号化して保存するべき債務を負っていたとは言えないとした理由。

(1) **経済産業省の告示等をみても、**重要な情報やデータについては**暗号化することが望ましいという指摘をしているだけ**であること。

(2) **IPAの文書では、**データベース内の全てのデータに暗号化処理を行う事は、サーバー自体の負荷になることがあるため、**特定のカラムのみ暗号化する等の考慮が必要であると指摘している**こと。

(3) **暗号化処理は、程度により**異なるものであり、それによって**被告の作業量や代金も増減する**と考えられること。

4. 判決の内容

- 被告の原告に対する説明義務違反は無いことから、債務不履行とはならないとした理由。

(1) SQLインジェクション対策を講じていないことは、債務不履行にあたるのであり、それとは別に信義則上の義務として当該内容を説明すべき義務を負うとは認められない。

(2) 流出原因がSQLインジェクションと認められる一方、その他のセキュリティ対策が脆弱であることが流出に寄与したことを認めるに足りる証拠がないため、セキュリティ対策が脆弱であることを説明すべき義務を負うとは認められない。

(3) サーバーのセキュリティレベルが最低であったことを裏付ける証拠がなく、説明義務を負うとする主張は前提を欠く。

(4) 原告は、**“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、一般的である”との説明を被告より受けており、危険性を認識していた**ことから、説明義務違反とは認められない。

4. 判決の内容

＜争点③：原告の過失と因果関係の断絶＞

裁判所の判断

原告が金種指定詳細化を依頼したこと、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仕様を放置したことは、債務不履行と流出との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。但し、被告から改修の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が流出の一因となった事は明らかであることから、当該過失を考慮し、3割の過失相殺をするのが相当とした。

4. 判決の内容

＜争点④:損害＞

裁判所の判断

原告の過失を考慮し、以下の合計金額である、3231万9568円から3割を控除した、2262万3697円を損害と認めた。

(1)本ウェブ受注システム委託契約に関連して支払った代金27万5625円
(2)顧客への謝罪関係費用1863万7440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
(5)Bデータセンター使用料42万円
(6)事故対策会議出席交通費4万7600円
(7)□□□応募フォーム変更6万3000円
(8)売上損失400万円

4. 判決の内容

＜争点⑤：損害賠償責任制限の合意の成否等＞

裁判所の判断

合理的に解釈すれば、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とした。しかし、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すべきであり、被告に重過失が認められる本件においては、適用されないとした。

4. 判決の内容

- 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とした理由。

（1）29条2項は、「損害賠償その他」について規定した第9章内に定められていることから、損害賠償に関する総則的規定と解される一方、25条は「機密保持」について規定した第7章内に定められていることから、**29条2項が原則として適用され、25条が「機密保持」に関して例外的に適用されるのは明らか**である。

（2）25条の「本契約内容に違反した場合」との記載は**誤記と認められ**、「本章の規定に違反した場合」と読み替えるべきである。

4. 判決の内容

- 29条2項が被告に故意又は重過失がある場合には、適用されないとした理由。

（1）被告に権利・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（故意に準ずる場合）にまで同条項により、被告の損害賠償義務の範囲が制限されることは、著しく衡平を害するものであること。

（2）29条2項を、相手方に故意又は重過失があった場合にまで適用することは、当事者の通常の意思に合致しない。

（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。）

4. 判決の内容

- 被告に重過失が認められるとした理由。

(1) 被告が展開する事業の一環として、ウェブアプリケーションを提供していることから、原告がその**専門的知見を信頼して委託契約を締結したと推認できる**こと。

(2) 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。**

(3) SQLインジェクション対策がされていなければ、第三者によるSQLインジェクション攻撃により、個人情報が流出する事態が生じ得ることは**予見が可能である**。

(4) **経済産業省及び独立行政法人情報処理推進機構が**、ウェブアプリケーションに対し、**SQLインジェクション対策をするよう注意喚起をしていたことから**、個人情報が流出する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**こと。

(5) **SQLインジェクション攻撃への対策を取ることに、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**、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こと。