損害賠償請求事件
東京地方裁判所判決／平成２３年（ワ）第３２０６０号
平成２６年１月２３日
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

主　　文

１　被告は，原告に対し，２２６２万３６９７円及びこれに対する平成２３年１０月１５日から支払済みまで年６分の割合による金員を支払え。
２　原告のその余の請求を棄却する。
３　訴訟費用はこれを５分し，その４を原告の負担とし，その余を被告の負担とする。
４　この判決は，第１項に限り仮に執行することができる。

事実及び理由

第１　請求
被告は，原告に対し，１億０９１３万５５２８円及びこれに対する平成２３年１０月１５日から支払済みまで年６分の割合による金員を支払え。
第２　事案の概要
本件は，原告が，被告との間で，原告のウェブサイトにおける商品の受注システムの設計，保守等の委託契約を締結したところ，被告が製作したアプリケーションが脆弱であったことにより上記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失し，原告による顧客対応等が必要となったために損害を被ったと主張して，被告に対し，上記委託契約の債務不履行に基づき損害賠償金１億０９１３万５５２８円及びこれに対する訴状送達の日の翌日である平成２３年１０月１５日から支払済みまで商事法定利率年６分の割合による遅延損害金の支払を求める事案である。
１　前提事実
（１）　当事者
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，保守受託及び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。
（２）　基本契約
原告（甲）と被告（乙）は，平成２１年１月３０日，業務委託基本契約（以下「本件基本契約」という。）及び覚書（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ついて定めたもの）を締結した。本件基本契約には，以下の条項がある。（甲３の１・２）
ア　第１章　総則
（ア）　第２条〔基本契約と個別契約〕
本契約は委託業務に関する基本的な事項について定め，別に締結される個々の取引に関する契約（以下「個別契約」という。）に適用されるものとする。
（イ）　第３条〔個別契約の成立〕
個別契約は次のいずれかにより成立する。
①　甲が注文書を乙に交付し，乙が注文書を受領したとき。
②　甲及び乙が別途書面により個別契約書を交わしたとき。
イ　第７章　機密保持

（ア）　第１７条〔対象情報〕

本契約の対象情報とは，文書，口頭及びデータを問わず，甲より乙，あるいは乙より甲に開示される企画，ソフトウェア，その他書類に記載され，若しくは電磁的又は光学的に記録された技術上，営業上その他業務上，一切の知識及び情報，及び第三者（個人及び法人）の名称・住所・電話番号・性別・年齢・生年月日・職業・クレジットカード番号・各種会員番号・各種パスワードをはじめとする第三者の属性に関する一切の個人情報であって，以下に該当するものを含み，かつ，これに準ずるもので双方が信義上守るべき事項。

①　機密である旨を「機密」「秘」「Ｃｏｎｆｉｄｅｎｔｉａｌ」等の表記によって明示しているもの。

②　口頭で開示した情報等については開示の時点において機密であることを明言し，かつ，開示の日から３０日以内にその旨を書面にて相手方に通知したもの。

③　書面・口頭以外の方法で提供又は開示された機密については提供又は開示の際に適宜「秘密」である旨の意思表示がされたもの。

④　甲の顧客に関する情報であって，提供又は開示の際に適宜「秘密」である旨の意思表示がされたもの。

（イ）　第１９条〔秘密保持義務〕

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）

（ウ）　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。

ウ　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）

エ　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）

（３）　ウェブ受注システムの発注

原告は，平成２１年２月４日，被告に対し，注文書を交付して，原告のウェブサイト「×××オンラインショップ」（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。）の導入を合計８８９万５６００円（消費税込み。以下では，特に断らない限り，消費税込みの金額を意味する。）で発注した（以下「本件システム発注契約」という。）。（甲４の１ないし４，乙３）

（４）　本件システムの利用

原告は，平成２１年４月末頃，本件システムの初年度利用料（平成２２年１月までの保守サービス料及びサーバー利用料）として，被告に対し，５７万７５００円を支払った。（甲５の１ないし３）

その後，原告と被告は，本件システムの利用（保守サービス及びサーバー利用）について，１年ずつ更新し，最後の更新では本件システムの利用期間が平成２３年２月から平成２４年１月までとされた。（乙６の１・２）

被告は，Ａ株式会社との間でサーバー利用契約を締結し，同社が設置したレンタルサーバー（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。

（５）　本件システムの完成及び引渡し

被告は，原告用にカスタマイズしたアプリケーション（以下「本件ウェブアプリケーション」という。）を製作して，本件システムを完成させ，平成２１年４月頃，原告による本件システムの検収を受けた。

原告は，同月１５日，本件ウェブサイトの稼働を開始した。この時点では，顧客（本件ウェブサイトを利用して商品を注文した者をいう。以下同じ。）がクレジットカードを利用して本件ウェブサイトで商品を注文する際には，顧客はカード会社が管理するウェブサイトの画面上でクレジットカード情報を入力するため，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。）に顧客のクレジットカード情報は送信されていなかった。

（６）　クレジットカード情報の保存開始

原告は，平成２２年１月頃，被告に対し，本件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，従前はクレジットカード決済，代金引換又は銀行振込みの区別しか原告では把握できていなかったため，原告の基幹システム側で請求元情報を正確に管理する目的から，各種クレジットカード種別（カード会社）を原告の基幹システムに送信する旨の本件システムの仕様変更（以下「金種指定詳細化」という。）を依頼し，同月２６日，注文書を被告に交付し，「機能カスタマイズ（金種指定詳細化）」を３１万５０００円で発注した。（甲８ないし１０，乙４）

被告は，同月２９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，同日に金種指定詳細化を導入した本件システムを稼働させた。同日以降は，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，本件サーバーにクレジット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クレジットカード情報のやり取りが行われるようになり，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。（甲８，２２の１・２）

（７）　ウェブサイトメンテナンス契約

原告（甲）と被告（乙）は，平成２２年５月１日，Ｗｅｂサイトメンテナンス契約（以下「本件ウェブサイトメンテナンス契約」という。）を締結した。本件ウェブサイトメンテナンス契約の契約書には，以下の条項がある。（甲３の３）

ア　第２条（保守サービス内容及び対象範囲）

本契約に基づき乙が甲に提供する保守サービスの内容は，別表記載のとおり（別表には，サイト更新，電話・メール・ＦＡＸでの問合せ対応が挙げられている。）とする。

イ　第４条（保守料及び支払方法）

甲は，保守サービスの対価として別表に定める保守料（別表には，年額３０万６０００円（消費税を除く）と定められている。）を支払う。

ウ　第１６条（損害賠償）

甲及び乙は，相手方が本契約に違反したことにより損害を被った場合，当該損害の賠償を相手方に請求することができるものとする。

（８）　顧客のクレジットカード情報等の流出

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した（以下「本件流出」という。）。

（９）　ＳＱＬインジェクションの意義等

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（又はＳＱＬインジェクション攻撃）とは，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。このＳＱＬ文を実行しないようにするための対策としては，バインド機構の使用及びエスケープ処理がある。

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。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。（甲２８）

２　争点及びこれに関する当事者双方の主張

（１）　争点①（本件流出の原因及び程度）

（原告の主張）

本件流出により，計１万６７９８件の顧客の個人情報（うちクレジットカード情報が含まれる件数は７３１６件）が流出した。本件流出の原因は，以下のいずれかである。

ア　ＳＱＬインジェクション

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（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。

イ　サーバーへのリモートログイン

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，更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。

ウ　管理機能への不正ログイン

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。事後の調査により，被告がＩＰアドレスによる接続制限を実施した日である平成２３年４月１１日よりも前の同月１日及び同月６日から７日に管理機能への不正ログインが行われたことが判明しているから，被告がＩＰアドレスによる接続制限をする前に管理機能への不正ログインがあった可能性は否定できない。

エ　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，利用者が悪意あるウェブサイトを閲覧したときに，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）が埋め込まれており，そのスクリプトが標的ウェブサイトへ転送され，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，当該スクリプトがブラウザで実行される攻撃である。

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頁が表示され，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。

（被告の主張）

本件流出の発生については認めるが，個人情報の流出件数は不知。

本件流出の原因は，以下のとおり，不明である。

ア　ＳＱＬインジェクション

本件流出に関して調査をした株式会社Ｂ（以下「Ｂ」という。）は，本件ウェブアプリケーションについて脆弱性があると指摘するが，その脆弱性があると指摘された部分はクレジットカード情報等の重要情報には何ら直結しない部分であり，その部分への攻撃により第三者が顧客のクレジットカード情報等の重要情報を取得できたことは何ら立証されて

おらず，Ｂ及び本件流出に関して別に調査をしたＣ社（以下「Ｃ」という。）も本件流出の原因を特定できていない。また，原告が指摘する「通信が成功したことを示すコード」とは，ウェブブラウザからのリクエストに対して本件サーバーが何らかのレスポンスをしたことにより，ウェブブラウザと本件サーバーとの間で通信が成立したことを示すものにすぎず，例えば，ＳＱＬインジェクション攻撃を本件システムがブロックしてエラー画面を表示させた場合でも，本件サーバーがエラー画面の表示というレスポンスをして通信が成立したことを示すために同じコードが表示されることがあり，上記コードは，ＳＱＬインジェクション攻撃が成功したことを示すものではない。さらに，原告は，ＳＱＬインジェクションによりいかなる情報が流出したかを具体的に特定していないのであって，ＳＱＬインジェクションにより第三者が顧客のクレジットカード情報等の重要情報を取得したとは認められない。

イ　サーバーへのリモートログイン

本件サーバーへのリモートログインＩＤ及びパスワードが不正に使用されたことを裏付ける証拠はない。

ウ　管理機能への不正ログイン

管理機能ログインＩＤ及びパスワードが不正に使用されたことを裏付ける証拠はない。また，被告は，本件流出発生前の平成２３年４月１１日までにＩＰアドレスによる接続制限を実施したから，本件ウェブアプリケーションの管理機能には，許可されたＩＰアドレスからしか接続できなかったので，管理機能への不正ログインが本件流出の原因である可能性は存しない。さらに，管理機能にログインしても，クレジットカード情報を閲覧及び操作することはできなかった。

エ　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が本件流出の原因であることを示す証拠はない。

（２）　争点②（被告の債務不履行責任の有無）

（原告の主張）

原告と被告は，本件基本契約（同日に締結した覚書を含む。），本件ウェブサイトメンテナンス契約及び本件基本契約に基づく各個別契約を締結しており，これらの契約は全て，被告が設計，開発，導入，変更，保守等を行う本件システムに関する一連の契約であって，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，上記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上記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，上記各契約は全て一体の契約（以下「本件ウェブ受注システム委託契約」という。）としてみるべきである。

そして，ウェブ受注システムは外部からの攻撃により顧客情報が流出する危険性があり，被告は，本件ウェブ受注システム委託契約に基づき，ウェブ受注システムの設計，運用及び開発を受託しているのであるから，システム開発，運用等の専門業者として以下の債務を負っていたが，その債務を履行しなかったことによる後記債務不履行１ないし５の責任を負う。

なお，被告は，本件流出の原因がＳＱＬインジェクションによる場合は，後記債務不履行１，３及び５の，本件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による場合は，後記債務不履行１ないし５の責任を負う（また，原告は明確に主張していないが，本件流出の原因がクロスサイトスクリプティングによる場合は，被告は後記債務不履行１の責任のみを負う旨主張するものと解される。）。

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）

被告は，自己が有する高度の専門的知識と経験に基づき，本件システムを設計及び開発した当時の技術水準として適切なセキュリティ対策が講じられたアプリケーションを提供すべき債務があった。被告が本件システムを設計及び開発した当時は，クレジットカード情報はサーバー上に保存することが予定されていなかったが，顧客の他の個人情報はサー

バー上に保存することが予定されていたのであり，ウェブ受注システムは外部からの攻撃により顧客の個人情報が流出する危険性があるから，その当時から，顧客の個人情報の流出を防止するためのセキュリティ対策が必要であったというべきである。

また，被告は，本件ウェブアプリケーション等がウェブ受注システムとして必要十分なセキュリティレベルとなるように，本件ウェブアプリケーション提供後も管理及び運用すべき債務を負っていた。

前記（１）の本件流出の原因は，いずれも一般的な攻撃方法であり，想定不可能な方法によるものではないから，被告には予見可能性があった。

（ア）　ＳＱＬインジェクション

被告は，ＳＱＬインジェクション対策として，ＳＱＬ文の組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てエスケープ処理を行うべき義務があったにもかかわらず，これらの対策を行わなかった。すなわち，プログラムの一か所にでもプログラム作成者の予想しないＳＱＬ文が実行される状態にあれば，第三者がクレジットカード情報等の個人情報を窃取することが可能であるため，ＳＱＬ文を構成する部分の一か所にでもバインド機構の使用又はエスケープ処理によるＳＱＬインジェクション対策がされていなければ，本件ウェブアプリケーションには脆弱性があり，被告の債務不履行を構成するというべきである。

（イ）　サーバーへのリモートログイン

被告は，インターネット上のウェブページを通じてリモートログインＩＤ及びパスワード並びにデータベースログインＩＤ及びパスワードが第三者に閲覧又は窃取されないように，適切なセキュリティ対策を講じたウェブアプリケーションを提供すべきであった。しかし，被告は，適切なセキュリティ対策を講じていなかったから，債務不履行を構成する。

（ウ）　管理機能への不正ログイン

被告は，インターネット上のウェブページを通じて管理機能ログインＩＤ及びパスワード並びにデータベースログインＩＤ及びパスワードが第三者に閲覧又は窃取されないように，適切なセキュリティ対策を講じたウェブアプリケーションを提供すべきであった。しかし，被告はセキュリティ対策を講じていなかったから，債務不履行を構成する。

（エ）　クロスサイトスクリプティング

被告は，本件ウェブアプリケーションについて，顧客のウェブブラウザ上でスクリプトを実行できないようにする対策を講じるべきであった。しかし，被告は，そのような対策を講じていなかったから，債務不履行を構成する。

イ　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）

被告は，本件システムを管理及び運用していたのであるから，第三者が本件サーバー，管理機能及び本件データベースにログインをすることを防止するために，本件サーバーに接続できるＩＰアドレスを制限し，ファイヤーウォール等を設置し，本件サーバーのセキュリティをアップし，又は本件サーバーの空きポートをチェックすべき債務を負っていた。

前記アのとおり，前記（１）の本件流出の原因は，いずれも一般的な攻撃方法であり，想定不可能な方法によるものではないから，被告には予見可能性があった。

しかし，被告は，上記債務を怠ったから，債務不履行を構成する。

ウ　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）

被告は，自己が有する高度の専門的知識と経験に基づき，クレジットカード情報の流出を防止する措置及びクレジットカード情報の悪用を防止できるような措置を講じるべき義務を負っていた。そして，被告は，原告からクレジットカード情報を保存することを依頼されておらず，これを保存しておく必要もなかったから，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。

しかし，被告は，上記債務を怠ったから，債務不履行を構成する。

エ　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）

被告は，本件サーバー，管理機能及び本件データベースへのログインＩＤ及びパスワードを第三者に推知されにくいものとし，定期的にパスワードを変更すべき債務及びパスワードを複数人で共有しないようにすべき債務を負っていた。

被告は，原告に対し，管理機能ログインＩＤ及びパスワードの変更方法を開示しなかったから，管理機能ログインＩＤ及びパスワードが推知されやすいもの（ログインＩＤが「ａｄｍｉｎ」，パスワードが「ｐａｓｓｗｏｒｄ」）であったことは，被告の債務不履行を構成する。

オ　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）

ウェブ受注システムにおいては，顧客が入力した個人情報が流出すると第三者による悪用の危険性が高いのであるから，システム設計，開発及び運用時の技術水準と同程度のセキュリティ対策を備えていることが求められる。また，システム設計，開発及び運用を行う業者は，情報システムの知識を有しない企業に対して，情報サービスを提供する専門家としての十分な配慮と注意を払う必要がある。

したがって，システム設計，開発及び運用を行う業者である被告は，発注者である原告に対し，原告が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うところ，ＳＱＬインジェクション対策を講じていないこと，本件システムのセキュリティ対策が脆弱であること，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，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といったセキュリティ対策の状態について一切説明しなかったことは，被告による債務不履行を構成する。

（被告の主張）

原告と被告との間では，本件基本契約，本件ウェブサイトメンテナンス契約その他の個別契約といった個々の契約が締結されているにすぎず，本件ウェブ受注システム委託契約といった包括的な契約は締結されていないため，被告の債務不履行の有無は，上記の個々の契約に基づく債務を前提として判断すべきである。そして，以下のとおり，被告には債務不履行がなく，また，仮に債務不履行があったとしても，被告には予見可能性（過失）が存しないのであるから，被告は債務不履行責任を負わない。

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）

被告が，原告との間で締結した契約の内容に従い，契約締結当時の技術水準に沿って，適切なセキュリティ対策が講じられたウェブアプリケーションを提供すべき債務を負っていたことは認めるが，本件ウェブアプリケーション等に関するセキュリティレベルを整備し続ける義務は負うことはない。

そして，被告が製作及び提供した本件ウェブアプリケーションは，その製作及び提供時の技術水準に照らし，品質及びセキュリティ水準に何ら問題がなかったのであるから，被告には，適切なセキュリティ対策が講じられたアプリケーションを提供すべき債務の不履行はない。セキュリティ対策は，コスト面と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り，製作されるプログラムの各箇所，その重要度に応じてセキュリティ対策レベルを分けることは当然のことであって，それを前提に「侵入されにくい」対策が採られていれば製作時点の義務履行としては必要十分である。特に，被告は，クレジットカード情報は一切取り扱わない仕様で原告から受注して本件システムを製作しているのであり，この点は本件システムの製作時点において講じられるべきであったセキュリティ対策レベルの判断における重要な要素となる。

また，原告が本件流出後に調査を依頼した大手調査会社（Ｂ）ですら，本件データベースへの侵入経路及び侵入手法は解明できていないから，本件流出は，専門業者の技術レベルを超える想定不可能な方法によって行われたものであり，被告にはその侵入行為について予見可能性がなかった。

イ　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）

本件システムにおいて，本件サーバーに接続できるＩＰアドレスを制限していなかったこと，ファイヤーウォール等のネットワークセキュリティー製品が設置されていなかったこと，ネットワークやサーバーのセキュリティ対策として，セキュリティ製品等を利用した特別の対策を講じていなかったことは，認める。

しかし，被告は本件ウェブサイトの変更権限を有しなかったために，原告の主張するセキュリティ対策を独断で講じることができる立場にはなく，原告との契約においても，被告が本件ウェブサイトのセキュリティ対策を講じる義務を負うことは規定されていなかったのであるから，被告は上記セキュリティ対策を講ずべき債務は負っていなかった。また，前記（１）のとおり被告は本件流出発生前の平成２３年４月１１日までにＩＰアドレスによる接続制限を実施していたし，Ｂ作成の報告書でも，サーバーには問題点が存しなかった旨が報告されており，被告による本件サーバーのセキュリティ対策が不十分であったとはいえないから，被告には債務不履行がない。

さらに，前記アと同じく，被告には予見可能性がなかった。

ウ　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）

原告は，金種指定詳細化の際，被告に対し，クレジットカード情報を顧客から取得し，本件データベースに保存した上で，原告がクレジットカード情報を利用できるように本件システムを変更することを依頼したのであって，被告がクレジットカード情報を保存せず，又は削除すべき債務を負っていたとはいえない。また，原告は，被告に対し，本件データベース上に保存する情報を暗号化することを委託していないし，暗号化の手法はデータの暗号化の程度や対象情報の範囲によって千差万別であるから，特に契約で暗号化が要求されていない以上は，被告がクレジットカード情報を暗号化すべき債務を負っていたともいえない。

エ　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）

被告が本件サーバー，管理機能及び本件データベースへのログインＩＤ及びパスワードを適切に設定及び保管していなかったことは否認する。管理機能へのログインＩＤ及びパスワードは，初期設定では原告の主張するとおりに設定されていたが（ログインＩＤが「ａｄｍｉｎ」，パスワードが「ｐａｓｓｗｏｒｄ」），後に原告が変更することを前提としていた上，平成２３年３月２９日，同年４月６日及び７日に本件ウェブサイトが不正アクセスを受けたことにより，同月８日に管理機能ログインパスワードを変更したのであって，被告による管理機能ログインＩＤ及びパスワードの設定及び保管にも不備はなかった。

なお，本件ウェブアプリケーションには本件データベースへのログインＩＤ及びパスワードが埋め込まれているため，仮に第三者がアプリケーションの操作を行えるようになった場合，本件データベースへのログインＩＤ及びパスワードを別に窃取していなくとも，本件データベースへのログインは可能であるから，本件データベースへのログインＩＤ及びパスワードの窃取は本件流出とは無関係である。

オ　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）

原告の主張する説明義務の発生根拠及び被告が説明すべき内容は明確でないし，原告は事業を営む企業であって消費者ではないのであるから，被告は，本件システムのセキュリティ対策について説明義務を負わない。

また，本件システムにはＳＱＬインジェクション対策を講じていないことによる脆弱性は存在しないこと，被告はＡ株式会社との間で通常の契約プランに基づきサーバーレンタル契約を締結しており，特にセキュリティレベルの低い契約形態を選択したものではないこと，原告は金種指定詳細化により，クレジットカード情報が本件データベースに保存され，普通に読み取り判別が可能な状態となったことを認識していたことから，被告には説明義務違反はない。

（３）　争点③（原告の過失と因果関係の断絶）

（被告の主張）

本件システムの運用当初には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ていなかったところ，原告は，自ら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することを被告に委託し（原告は，購入者のクレジットカード情報から，利用したカード会社情報を識別及び取得する仕様を求めたが，当時，その仕様を実現するためには，カード会社のシステムとの整合性上，本件システムがクレジットカード情報の全体を取得する以外に方法はなかった。），その後，その安全性及び改善の方法等に関して被告に質問をした際には，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，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仕様を放置したのである。そのため，本件流出の直接的原因は，原告の要望による金種指定詳細化のための本件システム仕様の変更にあり，原告が被告の上記指摘に対して何ら対応しなかったこと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ている。

（原告の主張）

被告は，原告の行為により，被告の債務不履行と本件流出との因果関係が断絶したと主張するが，原告は，金種指定詳細化以前は顧客が利用したクレジットカードのカード会社情報を取得せず，クレジットカード決済による売上全体額しか把握していなかったところ，被告に対し，各カード会社に対する毎月の売掛金額を個別に把握できるようにする旨の仕様変更を依頼したにすぎず，クレジットカード情報の取得及び保存を被告に依頼したものではないし（金種指定詳細化のために当然にクレジットカード情報全部を保存することが必要となるわけではない。），金種指定詳細化の際には，被告からは本件データベースにクレジットカード情報を保存する設定とする旨の説明を受けていなかった。原告は，その後の被告とのメールのやり取りにおいて，クレジットカード情報を保存する設定となっていることは認識したが，クレジットカード情報を暗号化していないこと及びクレジットカード情報をデータベース上で保存することの危険性を認識できなかったために，クレジットカード情報を保存せず，又は暗号化する設定への改修を求めなかったのであるから，かかる経緯からすると，原告の行為により被告の債務不履行と本件流出との因果関係が断絶するものではない。

（４）　争点④（損害）

（原告の主張）

原告が被告の債務不履行により被った損害は，以下の合計額１億０９５８万４８０９円である（なお，原告は，主張する損害額を訴状記載の金額よりも増額させたが，請求を拡張していないため，原告の主張する損害額の合計額は請求額を上回っている。）。

ア　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　２０７４万１１７５円（原告と被告が締結した契約の一覧表である別紙の各「受注額」欄記載の金額に消費税を加算して合計した金額に，更に別紙に記載が漏れている発注の代金７万３７６２円を加算した金額）

イ　顧客への謝罪関係費用　１９０２万１７９８円

（ア）　ＱＵＯカード及び包装代（１６７４万６７００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）
ウ　顧客からの問合せ等の対応費用　４９３万８４０３円
（ア）　コールセンター費用（４８６万６８４３円）
（イ）　コールセンターへの交通費（５８００円）
（ウ）　メール対応のための深夜帰宅タクシー代（６万５７６０円）
エ　調査費用　３９３万７５００円
（ア）　Ｃ　２２０万５０００円
（イ）　Ｂ　１７３万２５００円
オ　Ｂデータセンター使用料　４２万円
カ　事故対策会議出席交通費　４万８１００円
キ　□□□応募フォーム変更　６万３０００円
ク　売上損失　６０４１万４８３３円
（被告の主張）
不知。
（５）　争点⑤（損害賠償責任制限の合意の成否等）
（被告の主張）
ア　損害賠償金額制限の合意の成否
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。
イ　本件基本契約２９条２項の適用の有無
本件基本契約２９条２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から，被告に重過失があったとしても適用される。
また，本件システムにはＳＱＬインジェクション対策の不備はないこと，被告は，本件ウェブアプリケーション製作時点において，ＥＣ－ＣＵＢＥに関し公開されている必要な修正プログラムは全て適用を済ませた上で納品して検収を受けており，特に契約をしていない以上はその後に修正プログラムを適用する義務を負わないことから，被告には重過失は存しない。
したがって，被告の損害賠償義務は，本件基本契約２９条２項により，「個別契約に定める契約金額の範囲内」が限度となるところ，別紙記載の個別契約のうち，本件システムのセキュリティ対策に関する契約である別紙「契約番号」欄記載１（本件システム発注契約），９（プロジェクト名「×××モバイルサイト構築」）及び１２（プロジェクト名「×××モバイルサイト構築【２期制作】」）の各個別契約に係る代金の合計額が，被告が損害賠償義務を負う金額の限度となる。
ウ　責任期間制限条項の適用の有無
本件基本契約２６条２項は，被告の責任期間を，委託業務完了の後１年間と定めるものである。原告は，本件基本契約２６条２項は無償補修期間を定めたものにすぎないと主張するが，本件基本契約に基づく個別契約は請負契約としての性質を有し，請負契約では債務不履行責任の特則として瑕疵担保責任の規定が適用される以上，原告の本件請求も瑕疵担保責任の規定に従った請求というべきであるから，本件請求についても本件基本契約２６条２項が適用される。
したがって，仮に本件基本契約及びそれに伴う平成２１年２月４日発注の本件システム発注契約又は平成２２年１月２６日発注の金種指定詳細化に係る個別契約に関して被告に債務不履行が認められるとしても，本件基本契約２６条２項により，被告は損害賠償責任を負わない。また，平成２２年５月１日締結の本件ウェブサイトメンテナンス契約については本件基本契約２６条２項は適用されないが，被告は，本件ウェブサイトメンテナンス契約において，本件ウェブサイトに表示される内容の変更作業を受託したにすぎず，本件ウェ

ブサイトメンテナンス契約に基づいて本件ウェブサイトのセキュリティ対策を講じるべき義務を負うことはなく，本件ウェブサイトメンテナンス契約に基づく債務の不履行は存しないから，損害賠償責任を負わない。

（原告の主張）

ア　損害賠償金額制限の合意の成否

本件基本契約は，２９条２項では損害賠償金額の制限を定める一方，２５条では全額の賠償を定めるという矛盾する条項が併記されており，２９条２項が２５条の特則である旨は明記されていないし，２５条が，本件基本契約第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，当事者の合理的意思としては，民法の原則及び本件ウェブサイトメンテナンス契約１６条と同様に，相当因果関係がある損害全額の賠償を合意したものと解すべきであり，損害賠償金額を制限する旨の合意は成立していない。

また，損害賠償金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が，本件基本契約は，専門業者である被告が作成した定型的な契約書を使用したものであり，被告は原告に対して損害賠償金額を制限する２９条２項が２５条に優先して適用されるといった説明は一切していない上，本件基本契約は経済産業省が作成したモデル書式とは内容が異なるために，原告と被告との間では，本件基本契約２９条２項については個別的な合意は成立していない。

イ　本件基本契約２９条２項の適用の有無

本件基本契約２９条２項により損害賠償金額を制限する旨の合意が成立しているとしても，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。

そして，原告と被告が契約した当時，電子商取引システムにおいて代表的な攻撃手法であるＳＱＬインジェクション攻撃への対策を講ずべきことが周知されており，電子商取引システムの設計・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，被告は無償配布ソフトウェアであるＥＣ－ＣＵＢＥをベースとして本件システムを構築しており，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，被告は特にセキュリティ対策に注意すべきであったこと，ＥＣ－ＣＵＢＥについてはセキュリティ対策の修正プログラム（パッチ）が公表されており，ＥＣ－ＣＵＢＥの脆弱性を狙った攻撃に対処するためには，攻撃が行われる前に上記修正プログラム（パッチ）を適用する必要があるため，被告は，ＥＣ－ＣＵＢＥをベースとした本件ウェブアプリケーションについても同様の脆弱性が存在する可能性が高いことを容易に認識し得たのであり，原告との間で保守契約を締結して本件システムを管理及び運用していたのであるから，納品後も修正プログラム（パッチ）を適用し，又は原告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修正プログラム（パッチ）を適用していなかったことからして，被告には重過失が認められ，本件基本契約２９条２項は適用されない。

特に，本件では，原告と被告との間の契約実態がＡＳＰ（インターネットを介して，アプリケーションソフトをユーザーに提供するサービス形態）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，原告は被告がセキュリティ対策を行っていると誤信していたこと，被告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，前記（２）のとおり，被告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，被告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に許されない。

ウ　責任期間制限条項の適用の有無

本件基本契約２６条２項は，被告が行うべき無償補修の期間を定めたものであり，被告が負う債務不履行責任の期間を制限したものではない。なお，本件ウェブ受注システム委託契約は委任契約としての性質を有するから，被告の主張するように，債務不履行責任の特則として瑕疵担保責任の規定が適用されるものではない。

第３　当裁判所の判断

１　認定事実

前提事実に加え，証拠（以下の括弧内に掲げるもの）及び弁論の全趣旨によれば，以下の事実が認められる。

（１）　原告と被告との間での契約の概要

ア　原告と被告との間で締結された個別契約（以下「本件個別契約」という。）の内容及び代金（消費税抜き。以下，特に断らない限り，この（１）項において同じ。）は，別紙記載の契約番号１ないし５０，５２ないし７５，７７及び７８の各「プロジェクト名」欄及び「受注額」欄に記載されたもののほか，商品詳細画面改修等に係る発注（代金７万０２５０円）であり，本件個別契約の代金の合計額は１９７５万３５００円（消費税込みで，２０７４万１１７５円）である。（甲３７）

イ　原告は，本件ウェブサイトが稼働を開始した平成２１年４月分から平成２４年１月分まで，本件システムの利用料として月額５万５０００円を支払っており，うち２万５０００円がサーバー利用料，うち３万円が被告の標準保守サービス料であった。被告の標準保守サービスとしては，サーバー稼働確認，サーバー監視，サーバー障害対応及び原告からの問合せに対する対応業務を行う旨が定められていた。

また，原告は，本件システム導入当初には，本件ウェブサイトのデザイン変更作業を依頼する度に被告に料金を支払っていたが，平成２２年５月１日，本件ウェブサイトのデザイン変更作業を定額制とする内容の本件ウェブサイトメンテナンス契約を締結した。

（甲３の３，甲５の１ないし３，乙５，６の１・２）

（２）　本件システム等の概要

ア　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及びクレジットカード決済することをできるようにし，原告の売上げ及び在庫管理に関する基幹システムを本件ウェブサイトと連携させ，オンラインでの注文確定を可能とするシステムである。

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をカスタマイズしてＷｅｂ受注システムソフトウェア「△△△」を販売している。本件ウェブアプリケーションは，「△△△」を原告用にカスタマイズしたアプリケーションである。なお，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，被告は，クレジットカード情報を扱う機能を製作して本件ウェブアプリケーションに実装させた。

（甲６，乙７）

イ　本件システムのデータベースファイルは本件サーバー内（本件データベース）に保存されており，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。）も保存されることとなった。また，本件システムから原告の基幹システムに対して送信される情報は，金種指定詳細化の前までは，商品情報，顧客情報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のうちカード会社名も送信されることとなった。

ウ　一般的に，ネットワークを通じて，データベースに保存されている情報にアクセスしてその情報を閲覧するための方法としては，①データベースが保存されているサーバーにログインし，更に当該データベースにログインして，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，②インターネット上に公開されている通常のウェブページにおいて，意図的に不正な操作等を行うことで，当該ウェブページを制御している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権限なくデータベースに保存されている情報を読み出す方法，③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がある。原告が本件流出の原因として主張する事由のうち，サーバーへのリモートログインは①に，ＳＱＬインジェクションは②に，管理機能への不正ログインは③に該当する。

本件システムでは，インターネット回線を利用して本件サーバーにアクセスし，ＳＱＬを発行してデータベースを操作することが可能であり，金種指定詳細化の後は，データベースに直接ＳＱＬを発行することにより，クレジットカード情報を見ることができた。そのためには，本件サーバーにアクセスしてＩＤ及びパスワードを入力してログインし，更に本件データベースにアクセスしてＩＤ及びパスワードを入力してログインする必要があり，被告の従業員２名が上記各ＩＤ及びパスワードを知っていたが，原告は上記各ＩＤ及びパスワードを知らなかった。

（３）　金種指定詳細化に関する経緯

ア　原告は，金種指定詳細化以前は顧客が利用したクレジットカードのカード会社情報を取得せず，クレジットカード決済による売上全体額しか把握していなかったところ，平成２２年１月頃，被告に対し，各カード会社に対する毎月の売掛金額を個別に把握できるようにする旨の仕様変更を依頼した。これに対し，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，原告の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。そこで，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，本件システムに金種指定詳細化を導入するに際して，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，本件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。また，クレジットカード番号は，先頭の６桁の番号だけでカード会社を識別することができるが，本件データベースには，クレジットカード情報全部を保存する設定とされた。

（甲８，１０，５３，５４）

イ　原告担当者と被告取締役との間でのメールのやり取り

原告のシステム担当者であるＤ（以下「Ｄ」という。）は，原告が顧客のクレジットカード番号等を見ることができる設定となっていると認識した上で（ただし，実際には，上記のとおり原告の基幹システムにはカード会社名しか送信されず，原告が他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９月２７日，被告の取締役であるＥ（以下「Ｅ」という。）に対し，原告が顧客の個人情報を取得しないシステム構築の可否及び当該システム変更の費用を問い合わせた（以下のＤとＥのやり取りは，全てメールで行われている。）。これに対し，Ｅは，同月２９日，金種指定詳細化当時には，カード会社を判別するためにクレジットカード番号を取得する必要があったが，現在ではカード会社のシステム上で決済をした後にカード会社を判別することが可能となったことが判明したため，金種指定詳細化以前と同様の方式でカード会社名の情報を取得することができ，その方式に改修するための費用は２０万円程度である旨を伝えた。

Ｄは，同月３０日，Ｅに対し，原告が確認したところ，本件ウェブサイトでの注文がキャンセルになった場合及び電話で注文を受ける場合（商品の入荷数が少ないため，注文を受けられる客と受けられない客が発生して，本件ウェブサイトのカートが開けられない場合）にはクレジットカード番号を使用しており，「実際には，見え難い所にデータがあるだけで，全てのお客様のカード番号が，データとして保持されている。」と理解すればよいか，詳しくデータの流れを知りたい旨を伝えた。これに対し，Ｅは，同日，顧客が入力したクレジットカード情報はネットショップのデータベースに保存しているが，管理機能の画面上や管理者への通知メール文面等ではクレジットカード情報を表示させていないため，「データは保持しておりますが，事実上見ることは出来ないという状態です。」と伝えた。

Ｄは，同日，現状はデータベースにデータはあるが，データベースを直接見る手法を用いなければ番号は見られないことは了解した旨を伝えるとともに，イレギュラーな注

文に関しては電話連絡等でクレジットカード番号を聞くため，仕方ないことだと思うが，現状で問題がないか，インターネット上で販売している会社ではどのような管理になっているのが普通であるかを問い合わせた。これに対し，Ｅは，同日，「保持する／しないどちらのパターンもあり得ると思いますが，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。」と伝えた。

原告は，上記やり取りの後も，被告に対し，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。

（甲２の１・２，乙１の１・２）

（４）　本件流出発覚の経緯

ア　Ｆ株式会社（以下「Ｆ」という。）は，他のクレジットカード会社から，原告からクレジットカード情報が漏洩している懸念がある旨の情報を受けたことから，Ｆの会員でクレジットカードの不正利用被害を受けた者の過去の利用傾向を調査したところ，原告を利用していた会員が複数いたため，平成２３年４月２０日，原告に対し，上記の経緯を伝え，クレジットカード番号の保管状況を確認した。

原告は，Ｆに対し，業務運営においてクレジットカード番号データを見ないため，クレジットカード番号を保存していない旨回答した。

イ　株式会社Ｇは，同日，原告に対し，クレジットカードを不正利用された者が共通に利用している店舗が原告であることが確認された旨警告した。

これを受け，原告は，同日に本件ウェブサイトのサービスを停止し，同月２１日に本件データベースに保存されていたクレジットカード番号データを確認し，バックアップした後に本件データベースから削除した。

ウ　Ｆの会員で，過去に原告で利用したことがあるクレジットカード情報が同月１日以降に不正利用された件数（不正利用の可能性が高いとして決済されなかった件数を含む。）は，同月１日から１１日までは０件，同月１２日に１件，同月１４日に３件，同月１５日に４件，同月１８日に２件，同月１９日に１０件，同月２０日に５件であり，同月２１日以降も１日に複数件の不正利用が発生することがあった。

（甲２２の１・２，甲２６，２７，調査嘱託の結果）

（５）　セキュリティソリューションサービス事業を営むＢは，原告から本件流出の原因及び被害範囲の特定について依頼を受け，平成２３年４月２０日から同年５月９日まで調査を行い，以下の内容の調査報告書（以下「Ｂ報告書」という。）を作成した。（甲１２，１３）

ア　本件流出の発生日

平成２３年４月１４日

イ　原告の内部調査により判明した本件流出時の本件サーバー内での個人情報保持件数

個人情報が９４８２件，クレジットカード情報が６７９５件（同一顧客による注文を含むのべ件数では，７０１４件）。

ウ　ＳＱＬインジェクションの痕跡

一般的な攻撃の流れとして，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（事前調査）を行い，データベース情報を窃取する。

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をいう。以下同じ。）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。），また，後記カのウェブアプリケーション診断の結果，ＳＱＬインジェクションに対する脆弱性が確認された。

そのため，攻撃者が，事前調査によりデータベース情報等を窃取し，次に事前調査で得られたデータベース名等を悪用し，データベース内情報を窃取したと推測できる。被害件数は不明であるが，実害が出ており，３５３０件のＳＱＬインジェクション攻撃があるため，全件が漏洩した可能性が高い。

エ　管理機能への不正ログイン

管理機能への不正ログインは，平成２３年４月１日及び同月６日から同月７日までに中国から行われていた。攻撃者は，受注データ編集機能，受注情報ダウンロード機能，配送業者情報編集機能等にアクセスしていた。

そのため，攻撃者は本機能を悪用し，データの閲覧，改ざん及び取得を行った可能性がある。なお，ログインに必要なアカウント情報の窃取方法については特定に至っていないが，ＳＱＬインジェクションを悪用した場合，アカウント情報の窃取が可能である。

オ　ウェブアプリケーションへの攻撃

平成２３年３月２９日（ＰＯＳＴメソッドでのＳＱＬインジェクションが行われた日）のウェブページ出力用キャッシュから，攻撃者がアカウント情報，ウェブアプリケーションプログラム等を閲覧したと判断できるが，ウェブアプリケーションを動作させる権限ではパスワードファイルの読み込みができなかった。

カ　ウェブアプリケーション診断結果

平成２３年４月３０日に実施した本件ウェブアプリケーションに存在するセキュリティ上の問題の診断結果は，以下のとおりである。

（ア）　問題点１（個人情報が記載されたファイルの閲覧が可能）

本件ウェブアプリケーションでは，本件ウェブサイト内のアドレスにアクセスすることにより，アプリケーションのログファイルと思われるファイルの一覧が表示され，ログファイルの中に，氏名，メールアドレス，電話番号等を含む「お問い合わせ」内容が記載されていた。

上記問題点１のリスクレベルは，「Ｈｉｇｈ」（サイト及び利用者に重大な影響を及ぼし，サイトの社会的信頼性失墜につながると判断される問題であり，早急な対策が必要）である。

（イ）　問題点２（ＳＱＬインジェクション）

ＳＱＬ文として意味を持つ文字列を送信することにより，送信した文字がＳＱＬの一部として解釈された応答を確認した。診断実施期間内では任意の不正なＳＱＬ文の実行は確認できなかったが，応答の違いからＳＱＬ文を構成する方法に問題が存在すると判断することができる。

上記問題点２のリスクレベルは，「Ｍｅｄｉｕｍ」（間接的に攻撃に利用される可能性があり，複数組み合わせることで実害へと発展するため，対策が必要）である。

（ウ）　問題点３（クロスサイトスクリプティング）

ユーザーからの入力値に対してエスケープ処理が行われずに，そのまま次画面に出力されていたため，利用者のウェブブラウザ上でスクリプトを実行することが可能であった。

上記問題点３のリスクレベルは，「Ｍｅｄｉｕｍ」である。

（６）　Ｃは，原告から本件流出の原因，被害範囲及び本件流出に関連する証拠データ等の特定について依頼を受け，平成２３年４月２５日から同年５月９日まで調査を行い，以下の内容の調査報告書（以下「Ｃ報告書」という。）を作成した。（甲２２の１・２）

ア　漏洩／侵害の決定的な証拠の有無

調査対象となるサーバーのＡｐａｃｈｅ　Ｗｅｂログ，システム・ログ，ｆｔｐログ及び他の利用可能なシステム・ログを解析したが，データ漏洩／侵害の決定的な証拠はない。

イ　侵入日

不明

ウ　ＳＱＬインジェクション攻撃

攻撃者が平成２２年１２月１７日に本件サーバーに対して１５グループのＳＱＬインジェクションを実行し，平成２３年４月１４日に６２０個のＳＱＬコードを試行したことが確認されたが，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という証拠はない。

エ　悪意のあるソフトウェアのダウンロード試行

攻撃者が平成２３年３月２９日にインターネットから悪意のあるソフトウェアをダウンロードするためにクロスサイト・スクリプト攻撃を試みたことが特定されたが，悪意のあるソフトウェアが実際にダウンロードされたという証拠はない。

オ　操作ログ

本件システムでは，ＯＲＡＣＬＥデータベースの操作ログ機能を有効にしていないため，操作コマンドの履歴を追跡することができない。

カ　流出のリスクのあるクレジットカード・データ

合計７３１６件

（７）　本件流出後の本件ウェブサイトの状況

被告は，平成２３年４月２１日に本件サーバーを外部と遮断し，本件ウェブアプリケーションプログラム及び本件データベースを停止した。Ｂは，同月２２日に本件サーバー内のディスクの保存作業を実施した。本件システムは，同月３０日，被告により，Ｂのサーバーへの仮移行作業が行われ，Ｂにより安全性が確認されたため，同年５月から，クレジットカード決済を行わない状態で本件ウェブサイトにおけるウェブ受注が再開された。

そして，原告は，同年８月２３日，本件システムをＢの上記サーバーから株式会社Ｈのサーバーへ移行した上で，被告とは別の会社によって導入されたアプリケーションプログラムを使用して，クレジットカード決済を行うことが可能な状態でウェブ受注を再開した。（甲１１）

２　争点①（本件流出の原因及び程度）について

（１）　本件流出の原因

ア　前提事実のとおり，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，Ｆ及び株式会社Ｇが，同月２０日，原告に対し，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判断して警告を行ったこと（前記１（４）ア，イ）からすれば，同日までに本件流出が発生したと認められる。

そして，前記１のとおり，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（１（５）カ（イ）），一般的な攻撃の流れとして，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ところ，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が断続的に行われ，同年３月２９日及び同年４月１４日にＰＯＳＴメソッドによるＳＱＬインジェクション攻撃がされ，同日午前１０時３１分から同３６分までの５分間には海外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（１（５）ウ），Ｆの会員で，過去に原告で利用し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は，同月１日から同月１１日まで及び同月１３日は０件，同月１２日に１件にすぎなかったが，同月１４日から同月２０日までは１日に２件ないし１０件に増加したこと（１（４）ウ）が認められ，これらの事実に照らすと，同月１４日まで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，後記のとおり他に本件流出の原因が認められないことも考慮すれば，同日のＳＱＬインジェクション攻撃により本件流出が発生したと認めることができる。

イ　これに対し，被告は，Ｂ報告書においてＳＱＬインジェクションに対する脆弱性があると指摘された部分（本件ウェブサイトにおいて注文する商品の色選択画面と認められる。甲１３）について，クレジットカード情報等の重要情報には何ら直結しない部分であり，その部分への攻撃により第三者が顧客のクレジットカード情報等の重要情報を取得できたことは何ら立証されていない旨，Ｂが本件流出の原因調査の際に，本件流出について被告に責任があることを前提とした発言をするなどしたことから，Ｂは被告に対して不当な先入観を有しており，Ｂ報告書は信用性を欠く旨，Ｃ報告書でも本件流出の原因は特定されていない旨を主張する。

しかしながら，Ｂは，セキュリティソリューションサービス事業を営み，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（甲１９，２３），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ところ，Ｂ報告書もその専門的知見を利用して業務上作成されたこと自体により，一定程度の信用性が認められる。そして，前提事実及び証拠（甲２８）によれば，ＳＱＬインジェクション対策としては，プログラム作成者が想定していないＳＱＬ文を実行させないことが必要であるところ，本件ウェブサイトにおいて注文する商品の色選択画面では，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おらず，プログラム作成者が想定していないＳＱＬ文が実行される状態にあったこと，仮に他の場所にはＳＱＬインジェクション対策が実施されているとしても，１か所でもプログラム作成者の予想しないＳＱＬ文が実行される状態にあれば，その部分で攻撃者がプログラム作成者の予想しないＳＱＬ文の実行を繰り返すことにより，クレジットカード情報等の個人情報が格納された場所（テーブル名，カラム名等）を知ることが可能であること，その格納場所が判明すれば，ＳＱＬ文を実行することにより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のであり，本件ウェブアプリケーションには脆弱性があり，かつ，その脆弱性のためにクレジットカード情報等が全件漏洩した可能性がある旨のＢ報告書の記載部分は，プログラムに関する専門的知見に合致するものであり，信用することができる。

被告が主張する，Ｂが本件流出の原因調査の際に，本件流出について被告に責任があることを前提とした発言をしたなど，Ｂが被告に対して不当な先入観を有していたことを推認させる発言等の存在を裏付ける証拠はないから，Ｂ報告書が信用性を欠く旨の被告の上記主張は採用できない。また，Ｃ報告書は，データ漏洩／侵害の決定的な証拠はなく，侵入日は不明であると記載されているが，Ｂ報告書と同様のＳＱＬインジェクション攻撃の痕跡を指摘しているのであって，「決定的な証拠」，すなわち本件流出の原因を裏付ける直接証拠がないことを指摘するにとどまるから，ＳＱＬインジェクション攻撃が本件流出の原因であるとの推認をしたＢ報告書とは矛盾しないというべきである。

ウ　また，本件訴訟に係る事件は民事調停法２０条１項に基づき調停に付され，この事件について処理をした調停委員会（プログラムの専門家が調停委員に加わっている。）は，本件システムでは，ＯＲＡＣＬＥデータベースの操作ログ機能を有効にしていないため，外部者がいつ，どのような情報にアクセスしたのか不明である上，ＰＯＳＴメソッドが使用された場合には通信内容が一切記録されないため，外部者がＳＱＬインジェクションにより顧客のクレジットカード情報及び個人情報を取得したことを直接裏付ける証拠は存しないこと，流出した情報の内容及び流出時期が不明であって，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は，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を指摘した上で，直接証拠がない点を重視して，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おり（甲２８），被告も上記意見書と同様の点を指摘する。

確かに，本件流出の時期，程度又は原因を直接裏付ける証拠はないが，他方で，平成２３年４月に本件流出が発生したことは前提事実のとおりであり，何らかの方法により

本件データベースから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ことは動かし難い事実である。そして，上記意見書でも，サーバー内に保管されていたクレジットカード情報を含む個人情報を不正に取得するための方策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ところ，前記アのとおり，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日まで断続的にＳＱＬインジェクション攻撃が行われ，同日午前１０時３１分から同３６分までの５分間には海外ＩＰアドレスから１５０８回に及ぶＳＱＬインジェクション攻撃が行われたことは，同日まで断続的に事前調査が行われ，それによって本件データベース構造を把握した外部者が同日の短時間に相当数のＳＱＬインジェクション攻撃をしたことにより，本件流出が発生したことを推認させるに難くない。また，上記意見書が提出された後に行ったＦに対する調査嘱託の結果によれば，Ｆは，一般的に，同時期に複数会員において同じ傾向の第三者による不正使用（不正使用される店舗等が同一の場合等）が発生し，当該会員に過去共通の利用店舗があった場合，当該店舗がクレジットカード情報漏洩の発生源となっている可能性があると判断していること，本件では，第三者による不正使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ために原告に警告をしたのであり，原告以外の店舗には警告の連絡をしていないことが認められるのであって，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に基づくものといえるし，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存しないのであり，株式会社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をも勘案すれば，上記各カード会社の対応は，同月１４日の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を裏付けるものといえる。

以上からすれば，本件流出の原因は，ＳＱＬインジェクションであると認められる。

エ　次に，原告が主張する，他の本件流出の原因について判断する。

（ア）　サーバーへのリモートログイン

本件サーバーへのリモートログインＩＤ及びパスワードが第三者に流出したこと及び不正に使用されたことを裏付ける証拠はないから，サーバーへのリモートログインが本件流出の原因とは認められない。

（イ）　管理機能への不正ログイン

弁論の全趣旨によれば，管理機能へのログインＩＤ及びパスワードが第三者に推知されやすいものであったこと（ログインＩＤが「ａｄｍｉｎ」，パスワードが「ｐａｓｓｗｏｒｄ」）が認められ，前記１のとおり，平成２３年４月１日及び同月６日から同月７日に管理機能への不正ログインが行われたことは認められる（１（５）エ）。しかし，管理機能にログインした状態でクレジットカード情報を閲覧することができること及び管理機能への上記不正ログイン後にクレジットカード情報が閲覧されたことを裏付ける証拠はないから，管理機能への不正ログインが本件流出の原因とは認められない。

（ウ）　クロスサイトスクリプティング

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頁が表示され，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するが，かかる事実を裏付ける証拠はないから，クロスサイトスクリプティングが本件流出の原因とは認められない。

（２）　本件流出の程度

前記認定の事実によれば，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といわざるを得ず，また，Ｂ報告書とＣ報告書で，漏洩した可能性があると指摘するクレジットカード情報の件数が異なる理由は不明であるから，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。

３　争点②（被告の債務不履行責任の有無）について

（１）　原告と被告との間の契約関係

被告が負うべき債務の内容を判断する前提として，原告と被告との間の契約関係について検討すると，前提事実及び前記認定の事実によれば，被告は，原告との間で，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（本件システム発注契約），保守サービス（１年ごとに更新），クレジットカード情報の把握（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）等に係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ものと認められる（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。）。

これに対し，原告は，被告との間で締結した本件基本契約（同日に締結した覚書を含む。），本件ウェブサイトメンテナンス契約及び本件基本契約に基づく各個別契約は全て一体の契約としてみるべきであると主張するが，本件基本契約及び本件個別契約は別の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のであるから，これらの契約を全て一体の契約としてみて，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から，原告の上記主張は採用できない。

（２）　そして，前記２のとおり，本件流出の原因はＳＱＬインジェクションであると認められるから，本件個別契約及び本件基本契約に基づき，被告に債務不履行１，３及び５が認められるかを検討する。

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）

（ア）　前提事実のとおり，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。

そこで検討するに，証拠（甲１４，２５，２９）によれば，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うことができる。

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。

（イ）　被告は，原告が本件流出後に調査を依頼した大手調査会社であるＢですら，本件データベースへの侵入経路及び侵入手法は解明できていないから，本件流出は，専門業

者の技術レベルを超える想定不可能な方法によって行われたものであり，被告にはその侵入行為について予見可能性がなかったと主張する。

しかしながら，前記のとおり，被告が本件システム発注契約を締結した平成２１年２月４日時点で，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，ＳＱＬインジェクション対策として，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が必要であることが広く指摘されていたのであって，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被告において具体的に予見可能であったということができ，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に係る被告の予見可能性が否定されるものではない。したがって，予見可能性がなかったために過失がない旨の被告の上記主張は理由がない。

（ウ）　以上より，被告には債務不履行１の責任が認められる。

イ　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）

前提事実のとおり，原告は，平成２２年１月２６日に金種指定詳細化の業務を被告に発注しているが，その個別契約に基づいて，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いえるか検討する。

証拠（甲２４の１・２，甲２５）によれば，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）では，クレジットカード情報等（クレジットカード情報を含む個人情報）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，上記ＩＰＡの文書においては，データベース内のデータ全てに対して暗号化の処理を行うとサーバー自体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る（甲２５）ように，暗号化の設定内容等は暗号化の程度によって異なり，それによって被告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，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ない。

以上からすれば，被告には債務不履行３の責任は認められない。

ウ　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は，発注者である原告に対し，原告が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うと主張し，被告が説明すべき具体的内容としては，①ＳＱＬインジェクション対策を講じていないこと，②本件システムのセキュリティ対策が脆弱であること，③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，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としたことを指摘する。

しかし，上記①については，被告がＳＱＬインジェクション対策を講じていないことは，前記アのとおり，原告と被告との間での本件システム発注契約に基づき発生する，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（債務不履行１）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，被告が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義務を負うとは認められない。上記②については，前記２のとおり，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，その他の本件システム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はないから，被告が本件システムの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。上記③については，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を裏付ける証拠はないから，かかる事実は認められず，かかる事実を説明すべき義務を負うとする原告の主張は前提を欠くために採用できない。上記④については，前記１（３）イのとおり，原告のシステム担当者であるＤは，被告の取締役であるＥからの回答により，現状は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ことを認識していたことが認められ，被告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から，被告には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についての説明義務違反は認められない。

したがって，被告には，原告主張の説明義務違反が認められず，債務不履行５の責任は認められない。

４　争点③（原告の過失と因果関係の断絶）

（１）　因果関係の断絶について

被告は，本件システムの運用当初には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ていなかったところ，原告は，①自ら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することを被告に委託したこと（原告は，購入者のクレジットカード情報から，利用したカード会社情報を識別及び取得する仕様を求めたが，当時，その仕様を実現するためには，カード会社のシステムとの整合性上，本件システムがクレジットカード情報の全体を取得する以外に方法はなかった。），②その後，その安全性及び改善の方法等に関して被告に質問をした際には，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，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仕様を放置したことから，被告の債務不履行と本件流出との間の因果関係は，原告の上記各行為によって断絶された旨を主張する。しかし，金種指定詳細化以前から，本件データベースには顧客の個人情報が保存されていたのであり，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との関係でのみ因果関係が断絶するか否かが問題となるものと解される。

これを前提として被告の上記主張について検討するに，まず，上記①の点については，前記認定事実のとおり，金種指定詳細化の際，原告は，被告に対し，各カード会社に対する毎月の売掛金額を個別に把握できるようにする旨の仕様変更を依頼し，具体的には，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ことを要求したところ，被告は，金種指定詳細化以前の方式（カード会社が管理するウェブサイトの画面上でクレジットカード情報を入力する方式）では本件システムがカード会社名の情報を取得することができないため，金種指定詳細化の際には，本件サーバーにクレジットカード情報を入力し，その後本件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をする方式に変更したものと認められ，後者の方式によれば，その際に本件サーバーが顧客のクレジットカード情報を取得することはやむを得ないものの，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ない（カード会社名の把握のためにクレジットカード番号を保存するとしても，クレジットカード番号の先頭６桁の番号でカード会社を識別することができるのであるから，先頭６桁の番号を保存すれば足りる。）。そうすると，被告は，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は認められないにもかかわらず，これを保存する設定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って，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ものと解することはできない。

次に，記②の点については，前記認定の事実によれば，原告のシステム担当者であるＤは，被告の取締役であるＥからの回答により，金種指定詳細化以前と同様の方式（カード会社が管理するウェブサイトの画面上でクレジットカード情報を入力する方式）でカード会社名の情報を取得することができ，その方式に改修するための費用は２０万円程度であること，現状は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ことを認識していたことが認められる。しかし，ＥがＤに伝えているとおり，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ないのであって，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，その認識した後原告が被告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ものではなく，被告の債務不履行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いから，被告の主張する上記②の点は，債務不履行１と本件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。

（２）　原告の過失について

被告からは過失相殺の主張はないが，前記認定のとおり，原告のシステム担当者が，顧客のクレジットカード情報のデータがデータベースにあり，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いことを認識し，被告から本件システム改修の提案を受けていながら，何ら対策を講じずにこれを放置したことは，本件流出による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，原告に損害が認められるとしても，上記原告の過失を考慮し，３割の過失相殺をするのが相当である（上記の過失相殺事由は，因果関係の断絶を基礎付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。）。

５　争点④（損害）について

（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　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のであるから，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円が損害であると主張する。

しかし，原告は，本件ウェブサイトが稼働を開始した平成２１年４月１５日から株式会社Ｈのサーバー及び被告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，被告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，被告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，原告は，同年９月以降は被告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るところ，原告が上記のとおりサーバー及びアプリケーションを変更したことは，被告による債務不履行を受けて必要となった措置というべきであり，同年２月分から平成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（別紙契約番号６６。消費税抜き）のうち平成２３年９月分から平成２４年１月分の計２７万５６２５円（６３万円×５月／１２月×消費税１．０５）は，被告の債務不履行と相当因果関係のある損害と認められる。

（２）　顧客への謝罪関係費用　１８６３万７４４０円

顧客のクレジットカード情報を含む個人情報が漏洩するという事態が発生し，Ｂ及びＣからは，その漏洩件数は正確には不明であるが，全件（前記のとおり，最大で，個人情

報が９４８２件，クレジットカード情報が７３１６件で，合計１万６７９８件）が漏洩した可能性があると指摘されていたことからすれば，原告が，個人情報を登録していた顧客全員に対し，見舞金又は賠償金として一定の金員を支払い，顧客からの問合せに応じるなどの対応を行うことは，企業として必要かつ合理的な対応ということができ，基本的には，被告の債務不履行と相当因果関係を認めることができる（後記（３）項についても同じ。）。

ア　ＱＵＯカード及び包装代（１６３６万２３４２円）

証拠（甲３８の１・２，甲５２）によれば，原告は，本件ウェブサイトに登録していた顧客全員に対して本件流出のお詫びとしてＱＵＯカード１万６０３４枚を購入して送付し，ＱＵＯカードの代金及び包装代金として１６７４万６７００円を支出したことが認められるが，後記イ及びキによれば，原告が郵送したと認められるＱＵＯカードは計１万５６６６枚であるから，１６３６万２３４２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られる（１６７４万６７００円×１万５６６６枚／１万６０３４枚。小数点以下切り捨て。）。

イ　お詫びの郵送代（１２４万６４５９円）

証拠（甲３９の１ないし３，甲５２）によれば，原告は，上記アのＱＵＯカードを顧客に送付するため，１万５６６１通分の郵送代として１２４万６４５９円を支出したことが認められ，同額が被告の債務不履行と相当因果関係のある損害と認められる。

ウ　お詫び郵送に係る資材費及び作業費（８６万７１９６円）

証拠（甲４０，５２）によれば，原告は，上記アのＱＵＯカードを顧客に送付するために，資材費並びに封入及び宛名シール貼り等の作業費として８６万７１９６円を支出したことが認められ，同額が被告の債務不履行と相当因果関係のある損害と認められる。

エ　告知郵送代（８万１４４０円）

証拠（甲４１の１・２，甲５２）によれば，原告は，本件ウェブサイトに登録していた顧客のうち，電子メールを送信することができなかった顧客に対してお詫びの文書を郵送し，そのため１０１８通分の郵送代として８万１４４０円を支出したことが認められ，同額が被告の債務不履行と相当因果関係のある損害と認められる。

オ　告知の封筒代（１万０５００円）

証拠（甲４２，５２）によれば，原告は，上記エの文書を郵送するため，封筒１０００枚の代金として１万０５００円を支出したことが認められ，同額が被告の債務不履行と相当因果関係のある損害と認められる。

カ　お詫びのメール配信の外注費（６万６８４３円）

証拠（甲１１，４３，５２）によれば，原告は，本件ウェブサイトに登録をしていた顧客に対してお詫びの文書を電子メールで送信する作業（電子メールを送信できなかった際の調査作業等を含む。）を行わせるため，上記作業を外注し，その費用として６万６８４３円を支出したことが認められ，同額が被告の債務不履行と相当因果関係のある損害と認められる。

キ　お詫び及びＱＵＯカードの書留郵便代（２６６０円）

証拠（甲４５の１，甲５２）によれば，原告は，電話，電子メール及び郵便のいずれの方法によっても連絡を取ることができなかった顧客に対し，お詫びの文書及びＱＵＯカードを郵送するため，書留郵便を利用し，その５通分の代金として２６６０円を支出したことが認められ，同額が被告の債務不履行と相当因果関係のある損害と認められる。

ク　以上より，原告の主張する顧客への謝罪関係費用は，上記アないしキの合計額１８６３万７４４０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られる。

（３）　顧客からの問合せ等の対応費用　４９３万８４０３円

証拠（甲４４の１ないし３，甲４５の１ないし５，甲５２）によれば，原告は，本件流出への対応専用のコールセンターを設置するため，これを外注し，その費用として４８６万６８４３円を支出したこと，原告の従業員をコールセンターに待機させていたため，同従業員の交通費として５８００円を支出したこと，原告の役職員が深夜まで顧客へのメール

対応を行った後に帰宅する際のタクシー代として６万５７６０円を支出したことが認められ，いずれも被告の債務不履行と相当因果関係のある損害と認められる。

以上より，原告の主張する顧客からの問合せ等の対応費用合計４９３万８４０３円は，被告の債務不履行と相当因果関係のある損害と認められる。

（４）　調査費用　３９３万７５００円

前記認定の事実及び証拠（甲４６，４７）によれば，原告は，Ｃ及びＢに対して本件流出の調査を依頼し，その費用として，Ｃに対しては２２０万５０００円，Ｂに対しては１７３万２５００円を支払ったことが認められる。

そして，本件流出の原因等の調査には専門的知見を用いる必要があり，かつ，個人情報の漏洩という性質からは早急に調査を行う必要があるところ，Ｃ報告書とＢ報告書はそれぞれ記載内容が異なるように，ＣとＢはそれぞれが有する専門的知見を活かして報告書を作成したと認められることからすれば，本件流出の原因調査を上記２社に依頼したことが相当性を欠くとはいえず，上記調査費用は原告の本件流出への対応及び被告に対する損害賠償請求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いうべきであるから，上記調査費用の合計３９３万７５００円が被告の債務不履行と相当因果関係のある損害と認められる。

（５）　Ｂデータセンター使用料　４２万円

前記認定の事実及び証拠（甲４８の１・２，甲５２）によれば，原告は，平成２３年４月３０日から同年８月２３日まで，本件システムをＢのサーバーに仮移行しており，４か月分のＢのデータセンター利用料（サーバー利用料）として４２万円を支出したことが認められ，本件システムの仮移行という措置は，被告による債務不履行を受けて必要となった措置というべきであるから，同額が被告の債務不履行と相当因果関係のある損害と認められる。

（６）　事故対策会議出席交通費　４万７６００円

証拠（甲４９，５２）によれば，原告は，原告の東京本社で行う事故対策会議に宇都宮本社の従業員が出席するため，交通費として４万７６００円を支出したことが認められ（甲５２の陳述書には，交通費として４万８１００円を支出した旨の記載があるが，４万７６００円を超えて支出したことを裏付ける客観的証拠はなく，同陳述書の上記部分は採用できない。），かかる対応は，被告による債務不履行を受けて必要となったというべきであるから，同額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られる。

（７）　□□□応募フォーム変更　６万３０００円

証拠（甲５０，５２）によれば，原告は，上記（５）のとおり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□□□の応募フォームを変更する必要が生じたため，株式会社Ｉに対してその変更を依頼し，その費用として６万３０００円を支出したことが認められ，同額が被告の債務不履行と相当因果関係のある損害と認められる。

（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ったところ，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旨主張し，原告の従業員であるＪ管理部長作成の陳述書（甲５２）にもこれと同様の記載がある。

確かに，インターネット上での簡便な決済方法であるクレジットカード決済機能が利用できなかったことにより，本件ウェブサイトでも一定の売上減少があったことは推認することができるが，原告の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いない上，原告の損害額を算定する際には，売上減少に伴って支出を免れた仕入れ原価相当額等を控除する必要があるところ，本件ウェブサイトでは多様な商品が販売されていると推認で

き，売上げが減少した商品ごとの仕入れ原価等を立証することは極めて困難であると認められる。

以上の点を考慮すれば，上記期間（約４か月）の原告の売上損失としては，４００万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があると認めるのが相当である（民訴法２４８条）。

（９）　以上より，被告の債務不履行と相当因果関係のある損害は，上記（１）ないし（８）の合計３２３１万９５６８円となるが，原告が請求できる金額は，前記判示のとおり３割の過失相殺をするのが相当であるから，３２３１万９５６８円から３割を控除して，２２６２万３６９７円となる（小数点以下切り捨て。）。

６　争点⑤（損害賠償責任制限の合意の成否等）について

（１）　損害賠償金額制限の合意の成否

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。

これに対し，原告は，本件基本契約２５条が，「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旨主張するが，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ことは明らかというべきである（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。）。したがって，原告の上記主張は採用できない。また，本件ウェブサイトメンテナンス契約１６条では，「甲及び乙は，相手方が本契約に違反したことにより損害を被った場合，当該損害の賠償を相手方に請求することができるものとする。」と定められているが，本件ウェブサイトメンテナンス契約は，本件ウェブサイトのデザイン変更作業を定額制とする内容の個別契約であり，同条も，本件基本契約２９条２項の例外として，上記デザイン変更作業に関して被告が負担する損害賠償義務の金額が制限されないことを定めたものと解することができ，それ以外の損害賠償金額について本件基本契約２９条２項が適用されることを妨げるものとは解されない。

さらに，原告は，本件基本契約は専門業者である被告が作成した定型的な契約書を使用したものであること（甲１８），被告は原告に対して損害賠償金額を制限する２９条２項が２５条に優先して適用されるといった説明は一切していないこと（甲５１），本件基本契約は経済産業省が作成したモデル書式（甲３１）とは内容が異なることから，原告と被告との間では，損害賠償金額制限については合意が成立していない旨主張する。しかし，本件

基本契約の条項が定められた契約書は，原告及び被告が記名押印しており，その成立にも争いがないのであって，特段の事情がない限り，本件基本契約に規定されたとおりの契約が成立したものと認めるべきところ，原告の主張する上記の点は，上記のとおり解釈すべき本件基本契約２９条２項を含む契約が成立したことを否定すべき特段の事情に当たるものとはいえないから，原告の上記主張は採用できない。

（２）　本件基本契約２９条２項の適用の有無

ア　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（その従業員を含む。以下，この（２）項において同じ。）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。）。

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。

イ　次に，被告に重過失が認められるかを検討する。

（ア）　原告は，被告の重過失の評価根拠事実として，①電子商取引システムの設計・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，②被告は無償配布ソフトウェアであるＥＣ－ＣＵＢＥをベースとして本件ウェブ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，被告は特にセキュリティ対策に注意すべきであったこと，③被告は，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，又は原告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修正プログラム（パッチ）を適用していなかったことを主張するほか，④原告と被告との間の契約実態がＡＳＰ（インターネットを介して，アプリケーションソフトをユーザーに提供するサービス形態）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，原告は被告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被告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被告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，被告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に許されない旨主張する。

しかし，本件ウェブアプリケーションがＥＣ－ＣＵＢＥをベースとしていたことや，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）が適用されなかったことが，本件流出に寄与したことを裏付ける証拠はないから，原告の主張する上記②及び③の点は，原告の過失を基礎付けるものではない。また，上記④ないし⑥の点により本件基本契約２９条２項の適用が否定される法的根拠は明らかでない上，⑤被告がクレジットカード情報をログに記録する設定にしていたことは認められるが（甲３６の１），ログからクレジットカード情報が漏洩したことを裏付ける証拠はなく，

その他に本件システムに関するセキュリティレベルが極めて低いこと（ＳＱＬインジェクション対策が講じられていないという点を除く。）が本件流出の発生に寄与したことを認めるに足りる証拠はないこと，⑥前記のとおり，被告には説明義務違反が認められないことからすれば，上記④ないし⑥の点が，被告の重過失を基礎付けるものではない（ただし，被告が専門業者であるという点は，後記のとおり被告の注意義務の程度を基礎付ける要素となる。）。

（イ）　他方，上記①について検討するに，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ければ，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。

ウ　なお，本件基本契約１９条，２５条によれば，被告が本件基本契約１７条で定められた「対象情報」を原告の事前の書面による承諾なく第三者に開示又は漏洩した場合には，被告の損害賠償金額は制限されない。しかし，「対象情報」とは，「文書，口頭及びデータを問わず，甲より乙，あるいは乙より甲に開示される（中略）クレジットカード番号（中略）をはじめとする第三者の属性に関する一切の個人情報」であって，「機密である旨を「機密」「秘」「Ｃｏｎｆｉｄｅｎｔｉａｌ」等の表記によって明示しているもの」，「口頭で開示した情報等については開示の時点において機密であることを明言し，かつ開示の日から３０日以内にその旨を書面にて相手方に通知したもの」，「書面・口頭以外の方法で提供又は開示された機密については提供又は開示の際に適宜「秘密」である旨の意思表示がされたもの」，「甲の顧客に関する情報であって，提供又は開示の際に適宜「秘密」である旨の意思表示がされたもの」又は「これに準ずるもので双方が信義上守るべき事項」であり，その文言上，クレジットカード番号その他の個人情報であって，①原告又は被告から相手方に開示されたこと，②特に「機密」や「秘密」であることを明示されたことという要件をいずれも満たし，又は上記①及び②に準ずるものといえることが必要であると解されるところ，本件流出の対象となった顧客の個人情報又はクレジットカード情報は，原告から被告に開示されたものではなく，特に「機密」や「秘密」であることを明示したものでもないから，上記①及び②の要件をいずれも満たさず，上記①及び②に準ずるものともいえないから，本件流出について本件基本契約２５条は適用されない。

エ　以上より，被告には重過失が認められるから，本件基本契約２９条２項は適用されない。

（３）　責任期間制限条項の適用の有無

本件基本契約は，「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。」（２６条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。」（２６条２項）と定めている。

以上の規定からすれば，本件基本契約２６条２項は，被告による無償補修を定めた本件基本契約２６条１項を前提とした規定であり，被告が無償補修する義務を負う期間を原則として委託業務の完了後１年間とすることを定めたものと解することができ，原告の被告に対する損害賠償請求権の期間制限を定めたものと解することはできない。

これに対し，被告は，本件基本契約に基づく個別契約は請負契約としての性質を有し，請負契約では債務不履行責任の特則として瑕疵担保責任の規定が適用される以上，原告の本件請求も瑕疵担保責任の規定に従った請求というべきであるから，本件請求についても本件基本契約２６条２項が適用される旨主張する。しかし，本件基本契約２６条２項は，その文言上被告による無償補修期間を定めたものと解釈できることは前記説示のとおりであり，本件個別契約の性質が請負契約に当たるか，原告の請求が瑕疵担保責任に基づく請求といえるかといった点は，上記解釈に影響を与えるものではないから，被告の上記主張は採用できない。

第４　結論

よって，原告の請求は，被告に対し，債務不履行に基づき損害賠償金２２６２万３６９７円及びこれに対する訴状送達の日の翌日である平成２３年１０月１５日から支払済みまで商事法定利率年６分の割合による遅延損害金の支払を求める限度で理由があるから，その限度で認容することとし，主文のとおり判決する。

東京地方裁判所民事第４４部

裁判長裁判官　　脇　博人

裁判官　　木山智之

裁判官　　百瀬　玲