福岡工業大学研究論集 Res.Bull.Fukuoka Inst.Tech.,Vol.49 No.2 (2016) 69－86

基本判例研究

情報セキュリティ上の瑕疵による個人情報等の漏洩と個人情報保護法

―東京地裁平成 26 年 1 月 23 日判決の検討―

千 手 崇 史（社会環境学科）

Case Study;Leakage of Personal Information as a Result of Defects on Information Security and the Act on the Protection of Personal Information

―A Case of Tokyo District Court dated January 23,2014―

Takashi SENZU(Department of Socio-Environmental Studies)

Abstract

An interior wholesaler company(X:who ordered the system from Y)claimed system vendor company(Y). The legal basis is the default(Article 415,Civil Code). An enormous amount of personal data which X had been holding, leaked on account of illegal computer access by someone. Then,the system designed by Y didn't equip even minimum security guard. In this case,the Tokyo District Court partly upheld the claim. In case of information leakage incidents,companies suffer tremendous cost damage by voluntary apology to all customers. However, without apology,the social enterprise value falls. In this article,the author pointed out the "dilemma" problem.

Key words:personal information,default,business operator handling personal information,information leakage,Act on the Protection of Personal Information

［事案概要］

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，保守等の受託業務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東京地裁平成 26 年 1 月 23 日判決 一部認容，一部棄却判時 2221 号 71 頁

本件原告（X社という）は，インテリア商材の卸小売，通信販売などを行う株式会社である。本件被告（Y社という）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。

本件は，X社がY社に発注して構築したウェブサイトによる商品受注システムに不備があったことにより，顧客のクレジットカード情報などが流出した点について，X社が

平成 28 年 10 月３日受付Ｙ社に対して債務不履行に基づく損害賠償責任を追及した事案である。具体的な事案の流れは以下の通り。

平成 21 年１月，Ｘ社とＹ社は業務委託基本契約を締結し，この契約に基づいて，同年２月にＸ社のウェブサイトにおける商品受注システム（以下，本件システムという）をＸ社がＹ社に発注した（価格は 889 万 5600 円）。Ｙ社はＸ用に特化したアプリケーションを製作したうえで本件システムを完成させ，納品した後，Ｘ社とＹ社は本件システムの利用契約も締結した（併せて，Ｙ社は訴外Ａ社との間でサーバー利用契約も締結し，データーレンタルサーバー（以下，本件サーバーという）内に保存した）。

このシステムは，顧客の決済情報として，「クレジットカード決済」「代金引換」「銀行振込」しか把握できないシステムであった。平成 21 年４月の，本件ウェブサイトの稼働開始時には顧客のクレジットカード情報は本件サーバー内のデータベースに送信されていなかった。なお，判旨の部分で引用するが，当時は SQL インジェクションと呼ばれる不正アクセスの手法により個人情報などが流出する被害が多数生じていたため，独立行政法人情報処理推進機構（IPA）がそれへの対策として「バインド機構・エスケープ処理」の方法を用いることを推奨しており，経済産業省がこの IPA の推奨する方法を用いるように注意喚起もしていたが，Ｙ社の提供したプログラムにはこのような措置が施されていなかった。

平成 22 年１月，Ｘ社は顧客の決済情報を，顧客のクレジットカード情報の詳細（カード会社名，カード番号，有効期限，名義人，支払回数，セキュリティコード）まで正確に記録する目的で，顧客の各種クレジットカード情報をＸの基幹システムに送信する本件仕様変更（金種指定詳細化）をＹ社に依頼し，Ｙ社の完成，納品後に変更後の本件システムを稼働させた（仕様変更の価格は 31 万 5000 円）。その際，顧客のクレジットカード情報は暗号化されないまま，本件データベースに保存されていた。

その後，平成 22 年５月，本件ウェブサイトのメンテナンス契約を締結していたところ，平成 23 年４月に顧客のクレジットカード情報の不正使用が確認され，本件サーバーに外部からの不正アクセスがあり，クレジットカード情報を含む個人情報（購入商品，氏名，住所，電話番号，メールアドレス，パスワード等）が流出した（以下，本件流出という）ことが疑われた。なお，最大で，個人情報は 9842 件，クレジットカード情報は 7316 件，本件流出によって外部に漏洩した可能性があるほか，本件流出における外部からのアクセスは痕跡が残らないような方法でなされていた。

本件流出により，Ｘ社は顧客に対して謝罪，QUO カードの送付を行ったり，調査を実施することなどの積極損害が生じたほか，売り上げが減少するなどの消極損害が生じたため，Ｙ社に対して委託契約の債務不履行責任を追及し，１億 913 万円あまりの損害賠償請求をした。

裁判においては，⑴流出の原因・程度，⑵Ｙ社の債務不履行責任の有無，⑶Ｘ社の過失と因果関係の断絶，⑷損害，⑸損害賠償責任制限の合意と重過失の有無が争点とされた。こと，⑵との関連で，①適切な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カード情報を暗号化する債務の不履行，③セキュリティ対策に関する説明義務違反などが問題とされている（争点の（）数字，〇数字は筆者が付した）。加えて，本件業務委託基本契約の第 29 条２項に，Ｙ社の支払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」に制限する責任制限条項が設けられており，これの解釈も問題とされている。

［判決要旨］　一部認容，一部棄却

本判決は，結論としてＸの請求を 2262 万円の限度で認容し，その余を棄却した。

⑴　流出の原因・程度

Ｘ側から複数の流出原因が主張されていたが，本判決は，アクセスログに記録されない（痕跡が残らない）形で SQL インジェクション攻撃がなされたことが原因であると認めた。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，三菱 UFJ ニコス及び株式会社ジェーシービーが，同月 20 日，Ｘ社に対し，Ｘ社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（中略）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。」

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。」

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。（中略）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。（中略）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」

⑵　Y社の債務不履行責任の有無

前提として，債務は基本契約に包含されるものを一個と見る（※X社の主張）か，そこから派生した個別契約ごとに債務を観念するかという争点があったが，締結された時期が異なること，個別契約ごとに債務内容が異なることなどから，裁判所は（後者の）個別的にみる見解をとった。

① 適切な対策がとられたアプリケーションを提供すべき債務の不履行

以下引用するとおり，裁判所は，バインド機構を使用し，エスケープ処理が行われたプログラムを構築（※当時経産省が推奨していた）する債務を負っていたが，それが行われていなかったことを指摘し，債務不履行責任を認めた。

Y社は，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社は，当該個人情報の漏洩を防ぐために必要なセキュリティ対策を施したプログラムを提供すべき債務を負っていたと解すべきである。」

経済産業省は，平成18年2月20日，「個人情報保護法に基づく個人データの安全管理措置の徹底に係る注意喚起」と題する文書において，SQLインジェクション攻撃によってデータベース内の大量の個人データが流出する事案が相次いで発生していることから，独立行政法人情報処理推進機構（以下「IPA」という。）が紹介するSQLインジェクション対策の措置を重点的に実施することを求める旨の注意喚起をしていたこと，IPAは，平成19年4月，「大企業・中堅企業の情報システムのセキュリティ対策～脅威と対策」と題する文書において，ウェブアプリケーションに対する代表的な攻撃手法としてSQLインジェクション攻撃を挙げ，SQL文の組み立てにバインド機構を使用し，又はSQL文を構成する全ての変数に対しエスケープ処理を行うこと等により，SQLインジェクション対策をすることが必要である旨を明示していたことが認められ，これらの事実に照らすと，Y社は，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。」

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（中略）から，Y社は上記債務を履行しなかった」のであり，債務不履行責任を負う。

なお，Y社は，大手調査会社ですら侵入経路・手法を解析できておらず，専門業者の技術レベルを超える方法であったため，予見可能性がなかったとの主張をしていた。これに対して，裁判所は，契約時点でSQLインジェクション攻撃の事例が多数存在し，バインド機構，エスケープ処理の必要性が広く指摘されていたことから，予見可能性は否定されないとして，Y社の主張を排斥した。

② カード情報を暗号化する債務の不履行

一方，この債務に関して，IPAが暗号化を「望ましい」と述べていたに止まり，暗号化すべき債務までは負っていなかったと結論づけた。

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」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（中略）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。」

③ セキュリティ対策に関する説明義務違反

Ｘ社はＹ社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っていたと主張していた。裁判所は前記「セキュリティ対策を施したプログラムの提供義務の不履行」に当たると解釈し，それとは別個に信義則上の説明義務を負わないと判示した。

⑶　因果関係の断絶

Ｘ社が金種指定詳細化をＹ社に依頼した際，顧客のクレジットカード情報が本件データベースに保存されるように仕様変更を委託したのはＸ社なのであり，Ｙ社が質問した際にもその仕様を放置したのであるから，仮にＹ社に債務不履行があっても因果関係が断絶する，という主張をＹ社はしていた。これに対して，裁判所はクレジット番号を識別するには上６桁で足りるのに全部保存することとしたのはＹ社であること，流出の原因はSQLインジェクション対策を怠ったＹ社の債務不履行による危険の現実化といえることから，因果関係は断絶されないと判示した。もっともＸ社側も「顧客のクレジットカード情報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ほうが良いことを認識」していたため，それも情報漏洩の一因となっていることを考慮し，Ｘ社側に３割の過失があるものとして過失相殺をするのが相当であると判示した。

⑷　損害

裁判所は，［損害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，［損害２］顧客への謝罪関係費用　1863 万 7440 円，［損害３］顧客からの問合せ等の対応費用　493 万 8403 円，［損害４］調査費用 393 万　7500 円，［損害５］ラックデータセンター使用料　42 万円，［損害６］事故対策会議出席交通費　４万 7600 円，［損害７］リクナビネクスト応募フォーム変更　６万 3000 円 ，［損害８］売上損失 400 万円　という合計８項目の損害が，前記Ｙ社の債務不履行と相当因果関係のある損害であるとした。

その合計額は 3231 万 9568 円であるが，原告Ｘ社側に３割の過失があるとして過失相殺をなし，2262 万 3697 円が損害額であるとした。Ｘ社側の過失の内容は，「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」点である。

⑸　損害賠償責任制限の合意と重過失の有無

最後に，脚注 に掲げた契約条項の解釈が争われている。特に，29 条２項が損害賠償の免除を定めているため問題となる。Ｙ社は，第 25 条が損害賠償責任の発生根拠（民法の原則），29 条２項がその損害賠償金額の制限であると主張した。これに対して裁判所は，「本件基本契約は，29 条２項で，Ｙ社のＸ社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，Ｙ社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。」と判示した。29 条２項が「第９章 損害賠償その他」に規定されているため損害賠償の総則規定であり，25 条は「第７章 機密保持」に定められていることから例外に当たると解釈されることが理由として挙げられている。

次に，本判決は，ソフトウェア開発に関連して生じる損害が多額に上るため，その責任を制限することとした 29 条２項には一定の合理性があることを認めつつも，民法 572 条，640 条や基本契約 29 条２項の趣旨を手がかりとして，「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Ｙ社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（中略）本件基本契約 29 条２項は，Ｙ社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」と述べる。

最後に，Ｙ社に重過失があったか否かが問題となるが，Ｙ社がプログラムの専門的知見を活用した業務を展開し，Ｘ社がそれを信頼して発注をしていることから，Ｙ社の注意義務は「比較的高度なもの」とされた。続けて，経産省がバインド機構・エスケープ処理の注意喚起を行っていたことから本件事態が生じうることは容易に予見できた点，それら措置を行うことに多大な労力や費用がかかることもない点を理由として，Ｙ社には「重過失が認められる」と判示した。以上の判示内容をもとに，Ｙ社が 2262 万 3697 円（＋商事法定利率による遅延損害金）の賠償責任を負うと結論づけた。

なお，これにより判決は確定している。

［検討］判決の結論に賛成する

１. はじめに

1.1. 題材と検討方法

近年，企業活動においても情報の重要性が急激に高まっている。様々な情報を収集・保有・管理せずには企業は活動をすることができないが，情報は一度漏洩すると一方的に拡散を続けるほかなく，その間に会社や関係者に莫大な損害を及ぼし続けるため，企業はその漏洩防止や漏洩時の対応ということに重大な関心を持たざるをえない 。

さて，企業の保有する情報は無数に存在するが，特に重要なものとして営業秘密に関する情報と，顧客の個人情報を挙げることができよう。前者はライバル企業などに漏洩してしまうと漏洩元企業の長年の研究が無駄になる，当該企業が大きな損害を受ける，競争上不利な立場に置かれる等の事態が生じることになること等から，不正競争防止法（２条１項４号～９号，３条，４条，14 条等）により一定の保護がなされている他，秘密保持契約を従業員や関係者との間に結ぶなどの方法により保護をはかる企業も多い。

一方，個人情報にも後述するとおり，住所や氏名などの情報からクレジットカード番号や購買履歴など様々な情報が含まれる他，近年保護される（ひいては保有企業が取扱いに注意をしなければならない）情報の範囲が広い。これらを漏洩してしまうと企業の信用が落ちるだけでなく，顧客への謝罪対応に多大な時間と費用をかけなくてはならなくなる他，顧客から損害賠償などの訴訟を提起されるリスクも大きい。

このように，特に保護すべき情報として，営業秘密と個人情報を観念できるが，本稿は後者に関する事例を取り扱う。個人情報が漏洩した場合の損害が深刻であると考えられ，検討の必要性が高いからである。また，営業秘密に関しては，機械を製造販売する会社（機械やプログラム），食品の会社（売り方やノウハウ），製薬会社（薬品の化学式）など，業種によって内容も価値も多様であるのに対して，個人情報はある程度画一的に考えることができ，どの会社にとっても参考になる内容が多いと考えられ，研究の取りかかりとして適当であると考えられたからである。営業秘密に関しては後日機会があれば検討したい。

次に，個人情報漏洩の問題にも，漏洩予防の仕組み（内部統制システムや個別契約における漏洩防止義務），漏洩時の責任（会社の債務不履行・不法行為責任，役員等の損害賠償責任），漏洩後の処理（マスコミ対応や個人情報漏洩保険）など様々な段階を観念しうるが，本稿が取り上げた東京地判平成 26 年１月 23 日（以下，本判決という）は情報漏洩の金銭的処理（債務不履行責任）が問題とされている。予防の仕組みや漏洩後の処理の問題に関しては，機会を改めて取り組みたい。

1.2. 企業保有個人情報の漏洩事件

本稿が特に問題とする「企業からの個人情報漏洩」に関わる事件は多数存在する。ほとんどすべての事案は，現行「個人情報保護法」（後述）に違反しうるが，個人情報保護法には責任規定がないため，漏洩により損害を被った顧客等は，債務不履行や不法行為の規定を用いて損害賠償を請求する（とはいえ，そのパターンは様々である）。さしあたり，最近の個人情報漏洩事件の中で，特に大規模なものとして，以下の２種類を紹介する。

1.2.1.（共同）不法行為の事案―Yahoo!BB 事件

（大阪地判平成 18 年５月 19 日判時 1948 号 122 頁）

（事案）「Yahoo BB」の名称を用いて非対称加入者伝送（ADSL）方式を用いたインターネット接続サービスを展開する Y1 社・Y2 社はＸらとインターネット接続サービスに関する契約を締結し，その者らの個人情報を保有・管理するに至った。当該個人情報は当初 Y2 敷地内に設置されているサーバーに記録されていたが，平成 14 年２月，社外のパソコンからメンテナンス作業を行うために，「リモートメンテナンスサーバー」を設置し，社外のパソコンから社内のサーバーにリモートアクセスをすることを可能にしていた。具体的に，メンテナンス等を行う際は，①社外のパソコンからリモートメンテナンスサーバーにアクセス ② ①の際，ユーザー名とパスワードを正しく入力すると，ユーザー認証を受けて同サーバーにログオンできる ③その後，社内の各サーバーに接続する ④③の際も，さらにユーザー名とパスワードが必要となる という仕組みであった。ここで，ＡはY1 の業務委託先から Y1 へ派遣され，Y1 の顧客データベースサーバーの管理業務等に従事しており，前記ログオンに必要なユーザー名とパスワードをそれぞれ付与されていた者である。このＡは業務を終えた後，ユーザー名とパスワードがまだ利用可能であることを奇貨として，知り合いのＢとともに，ネットカフェ（インターネット接続可能な休養施設）のパソコンから Y1 の顧客データベースにリモートアクセスを行い，顧客情報を不正取得した。これに関して，個人情報を流出させられた顧客Ｘらが，Y1 社らに対して不法行為に基づく損害賠償請求をした。なお，Y1 社らがＡの業務が終了した後も，ユーザー名やパスワードの削除やパスワードの変更を行わず，またリモートメンテナンスサーバーの設置から１年間，パスワードの定期的な変更も行っていなかったことが「過失」に当たるか否かが問題とされた。

裁判所は，個人情報保護法 20 条（ただし，本件不正取得当時は施行前）の規定を指摘し，電気通信事業者である Y1 社らが個人情報漏洩防止などに関して必要な措置をとる注意義務を負っており，「リモートアクセスについては，JIS 規格や，コンピュータ不正アクセス対策基準（平成８年通商産業省告示第 362 号）で，その危険性が指摘され，不正アクセスへの対策について各種の規定がされているところであり（規定の内容については被告らも争わない。），これらの規定等の存在が示すように，あるサーバーに対してリモートアク

セスを可能にすることは，それ自体，当該サーバーに対する外部からの不正アクセスの危険を高めるものであるといえる。

被告 Y2 は，個人情報の管理に関して（中略）本件顧客データベースサーバーについて，そもそも必要性がない場合又は必要性のない範囲にリモートアクセスを認めることは許されず，また，リモートアクセスを可能にするに当たっては，不正アクセスを防止するための相当な措置を講ずべき注意義務を負っていたというべきである。」

被告は「リモートアクセスの管理体制は，ユーザー名とパスワードによる認証以外に外部からのアクセスを規制する措置がとられていない上，肝心のユーザー名及びパスワードの管理が極めて不十分であったといわざるを得ず，同被告は，多数の顧客に関する個人情報を保管する電気通信事業者として，不正アクセスを防止するための前記注意義務に違反したものと認められる。」

その上で，不正取得の予見可能性も結果回避可能性もあったことを認め，不法行為責任を認めた。

なお，流出した情報は〔１〕住所〔２〕氏名〔３〕電話番号〔４〕メールアドレス〔５〕ヤフーID〔６〕ヤフーメールアドレス〔７〕申込日などであったが，「個人の識別等を行うための基礎的な情報であって，その限りにおいては，秘匿されるべき必要性が高いものではない。」としながらも，「しかし，このような個人情報についても，本人が，自己が欲しない他者にはみだりにこれを開示されたくないと考えることは自然なことであり，そのことへの期待は保護されるべきものであるから，これらの個人情報は，原告らのプライバシーに係る情報として法的保護の対象となるというべきである。」としてその要保護性を認め，Y1 らの過失によりＸらのプライバシー権が侵害されたことにつき，一人あたり 6000 円（慰謝料 5000 円，弁護士費用 1000 円）の限度で認容した。

なお，判旨の中で個人情報保護法（詳しくは後述）が指摘されているが，事件当時成立のみしており，施行はされていなかった。その他，判決文からは，流出した情報は数百万件ともいわれ，争われているが，日弁連の調査によれば，660 万件程度である 。また，判決文には，原告らの人数と賠償の総額に関する正確な情報は見当たらない。

1.2.2.使用者責任の例―TBC 事件

（東京高判平成 19 年８月 28 日判タ 1264 号 299 頁）

（事案）この事件は，顧客Ｘらが，顧客情報の流出により損害を受けたとして，その顧客情報の管理等を行っていたＹ社を被告として損害賠償を求めた事案である。具体的に，被告Ｙ社（エステティックサロンを経営する会社）は，Ａ社との間でサーバーのレンタル契約を締結してウェブサイトを開設しており，その保守を委託していた。Ｘら顧客 14 名は，平成 12 年から 14 年の間にＹ社の無料体験に募集し，個人情報（後述）を登録していた。この時点ではＡ社により，これら個人情報が第三者からアクセスされないような設定がなされていた。しかし，ウェブサイトへのアクセスが増加したため，Ａ社がこれら個人情報を専用サーバーに移した際，インターネットにより第三者によるアクセスが可能な状態におかれてしまい，Ｘら 14 名の個人情報が流出したものである。なお，これにより流出した個人情報は，氏名，住所，年齢，性別，職業，電話番号，メールアドレス及びスリーサイズ・希望コース名などである。また，この流出によりＸらの個人情報がインターネット上の掲示板に掲載されたり，迷惑メールやダイレクトメールが届くようになるなどの被害が生じた。ＸらはＹ社に対して，不法行為または使用者責任（民法 715 条）に基づいて各々慰謝料
100 万円等の損害賠償の支払いを求めて提訴した。裁判所はＹ社が「本件ウェブサイトのコンテンツの具体的な内容を自ら決定し，その決定に従いＡ社が行ったコンテンツ内容の更新や修正について，セキュリティ等を含めてその動作を自ら確認していたものであり，また，Ｚ社から随時運用に関する報告を受け，障害や不具合が発生したときはＡ社と原因や対応等について協議していたことが認められるから，控訴人は，Ｚ社が行う本件ウェブサイトの制作，保守について，Ａ社を実質的に指揮，監督していたものということができる。」

また，本件で流出した情報の要保護性と損害額について，「本件において流出した情報がエステティックサービスに係るものであるところから，個々人の美的感性の在り方や，そうしたものに関する悩み若しくは希望といった個人的，主観的な価値に結びつく，あるいは結びつくように見られる種類の情報である点で，流出データ回収の完全性に対する不安ないしは精神的苦痛に対する慰謝料請求や，大学在籍に係る個人識別情報の開示に関する慰謝料請求につき判定されるべき場合よりは，通常，より高い保護を与えられてしかるべき種類の情報であると認められることにかんがみて，高額にすぎることはなく適切妥当であるというべきである。」と述べ，一人あたり３万 5000 円（慰謝料３万円，弁護士費用 5000 円）の限度で請求を認めた。これが低額すぎるかについて，「本件においては，前示した種類の情報の性質，流出の態様と程度に照らして，その損害額を認定すれば足り，個人情報の開示を明示的に反対したにも関わらず情報を開示した場合

や，ネット上で個人情報を開示して悪戯電話が多数かかってきた場合などと比べると，保護すべき個人情報の性質，具体的な２次流出あるいは２次被害の有無など前示した次第であることに照らして，前記各損害額は低額にすぎることはなく適切妥当である。」と述べている。なお，本事件発生当時（地裁への係属前）には，後述する個人情報保護法は施行されていない。

1.2.3.本事案の新規性

以上紹介した事案の特徴は，「個人情報の保有者がシステム開発等を専門とする業者等にシステムを委託し」それに伴い「主に当該受託者の過失（故意）により情報漏洩が起こった」点であろう。本件事案も，同様にシステム開発者の設計したシステムに不備があったことにより，クレジット番号等の情報が漏洩した点は同様である。

もっとも，紛争の態様をよく見ると全く異なる点を指摘できる。まず，Yahoo!BB 事件と TBC 事件は，当該個人情報を漏洩被害を受けた顧客との関係では，「保有者もシステム設計者も責任を負うべき」ものとなる。法的構成としては，不法行為（使用者責任や共同不法行為），債務不履行等様々なものがあるが，個人情報の主である顧客等が原告であり，個人情報を保有していた事業者も，システム設計に関わった者も被告の側に位置づけられる。このような対顧客との関係を本稿で「外部関係」と呼ぶとすれば，これまでの個人情報漏洩事件のほとんどはこの外部関係が問題となっている。それに対して，本件事案は，個人情報の保有者は顧客に対して先に謝罪や賠償，システムの改善等の対応を行っており，顧客と起こりうる紛争をあらかじめ処理している。そして，残った個人情報保有者がシステム設計者に，既にかかった費用（損害）の分担を求めることが紛争の実質をなしている（本稿ではこれを「内部関係」と呼ぶ)。その点が本事案の新規性であり，事例として紹介する価値が高いと思われる。予め様々な対応をしたＸ社は一部過失があるにせよ，おおむね真摯な対応をなしており，その後システム開発者たるＹ社から，費用損害の一部を賠償として勝ち取っていることから，今後同様の事態に巻き込まれた企業の対応や予測可能性などの点から，本判決は一定の参考となると思われる。

２.前提問題―プライバシー権と自己情報コントロール権

2.1.なぜこの問題を扱うのか

本件のような「個人情報漏洩」の事例を扱うためには「個人情報保護法」の規制・保護対象としている「個人情報」などに関する議論を避けて通れない。本判決において，直接に侵害されたのはＸ社の「財産や信用」であろうが，その前提として漏洩してしまった個人情報の主である個々人の利益が侵害されている。そして，明文で保護される「個人情報」の概念と「プライバシー権」の生成，変遷は深い関係がある。よって，本章において，まず「プライバシー権」の概念の生成にさかのぼって，そこから時系列に流れを見る方法をとる。

2.1.1.プライバシー権の生成―宴のあと事件最高裁判決

個人の住所や電話番号，カード情報，写真などの流出事件が大規模化してきたのは最近（インターネット発達後が特に多い）のことであるが，これら情報はそこで初めて保護されるようになったものではない。議論は，いわゆる「プライバシー」の権利（憲法 13 条）の発生や定着等にさかのぼる。ここで，保護されうるプライバシーの概念そのものが判例法上変遷しているため，それを簡単に確認しておきたい。そもそも，プライバシー権は明確な定義をもった権利ではなく，その内容は時代や社会の状況に応じても変化するものであるが，プライバシーの権利性に初めて正面から触れたものとして，有名な「宴のあと」事件判決を紹介することができる。政治家の私生活を「のぞき見」したかのようなモデル小説（私生活や性生活，感情の内面などが描写されていた）の出版により損害を被ったなどとして，被害者が出版社らを訴えた事件において，裁判所（東京地裁昭和 39 年 9 月 28 日下民集 15 巻 9 号 2317 頁 ）は，人格権に包摂されるプライバシー権が「私生活をみだりに公開されないという法的保障ないし権利」として理解され，私法的な権利性を持つことを確認した後，「公開された内容が（イ）私生活上の事実または私生活上の事実らしく受け取られるおそれのあることがらであること，（ロ）一般人の感受性を基準にして当該私人の立場に立つた場合公開を欲しないであろうと認められることがらであること，換言すれば一般人の感覚を基準として公開されることによつて心理的な負担，不安を覚えるであろうと認められることがらであること，（ハ）一般の人々に未だ知られていないことがらであること」を，私法上の救済の要件として掲げた。

2.1.2.プライバシー権と情報漏洩―宇治市住民票データ流出事件

上記「宴のあと」事件の理解は，個人情報漏洩の事件にも受け継がれている 。企業の個人情報の事例ではないが，リーディングケースとして，いわゆる宇治市住民票データ流出事件が重要である。これは，市が管理する住民基本台帳の情報を利用した乳幼児検診システムの開発を民間業者に委託したところ，その再々委託先のアルバイト従業員がこれら個人情報（氏名，年齢，性別，住所，家族構成などが含まれる）

を不正コピーし，名簿業者に転売するなどして，それら情報が結果的にインターネットに掲載されるなどした事件であり，被害を受けた市民らが原告となり，民法 715 条に基づいて市の責任が追及された。裁判所（大阪高裁平成 13 年 12 月 25 日 ）は，「本件データに含まれるＸらの個人情報は，明らかに私生活上の事柄を含むものであり，一般通常人の感受性を基準にしても公開を欲しないであろうと考えられる事柄であり，更にはいまだ一般の人に知られていない事柄であるといえる。」と，「宴のあと」事件の規範を引き継いで，プライバシー権としての要保護性を認めた。判決はさらに，インターネットで閲覧可能な状態になっていなくとも，法律上，市の適正な支配下におかれるべきこれら個人情報が「その支配下から流出し，名簿販売業者へ販売され，更には不特定の者への販売の広告がインターネット上に掲載されたこと，また，控訴人（※筆者注，「市」を指す）がそれを名簿販売業者から回収したとはいっても，完全に回収されたものかどうかは不明であるといわざるを得ないことからすると，本件データを流出させてこのような状態に置いたこと自体によって，被控訴人（※筆者注，「住民ら原告」を指す）らの権利侵害があったというべきである。」として，侵害の危険性がまだ具体化していない段階で権利侵害を認めている。なお，市と再々委託先のアルバイト従業員との間の実質的な指揮命令関係もあったとしており，当該従業員の選任・監督につき注意を怠ったとはいえないとして，市の使用者責任を認めた。以上のように，プライバシー権自体の要保護性はすでに判例上確立したものといってよい。

2.1.3.自己情報コントロール権―住基ネット訴訟

もっとも，近年はプライバシー権を「自己情報コントロール権」と位置づけ，より積極的な権利として位置づける見解も多い 。情報の漏洩ではなく，収集管理そのものが問題となった，いわゆる「住基ネット訴訟」最高裁判決が参考になる。住民基本台帳ネットワークシステムにより行政機関が住民の同意を得ずに本人確認情報を収集・管理・利用する行為が憲法 13 条に反するか否かが争われたことに関連して，最高裁（最判平成 20 年３月６日民集 62 巻３号 665 頁（判タ 1164 号 123 頁掲載)）は，「憲法 13 条は，国民の私生活上の自由が公権力の行使に対しても保護されるべきことを規定しているものであり，個人の私生活上の自由の一つとして，何人も，個人に関する情報をみだりに第三者に開示又は公表されない自由を有するものと解される」と判示している。通説はこれを「自己情報コントロール権」に関する判示であると理解している 。

主に公権力と私人という枠組みで，プライバシー権の概念は，このように「私生活をみだりに公開されない権利」という消極的な理解から，「自己情報コントロール権」という積極的な理解へと重点が移っていると考えられる。本稿が問題とする「プライバシー情報」「個人情報」は，私法的な問題であるが，やはりこれら権利を民事的な被侵害利益と捉え，目的外使用や漏洩，誤情報の訂正などの局面で私法的救済を与えるか否かを議論する流れは，特にプライバシーを「自己情報コントロール権」（積極的な請求権）と捉える見解と親和的であると考えられる。

2.2.個人情報保護法との関連

2.2.1.個人情報保護法の概要

上記「プライバシー」の要保護性は重要であるが，判例法上の権利であり，どの範囲までの情報が保護されるかは個別具体的に判断されていたようである。上記の通り，この概念自体まだ確立したものとは言いがたいが，それと並行して，個人の住所や電話番号，クレジットカードなどの情報の要保護性を考慮し，成文法として成立したのが「個人情報保護法 」である。本款では，個人情報保護法の概要に触れたい。

先述した宇治市住民票データ漏洩事件など，個人情報の流出事件が続発していたこと，また，民間部門の個人情報保護法制が存在していない事などを直接の理由として，同法は 2005 年に全面施行された 。個人情報保護法は，前半部分（第１章～第３章）が個人情報保護の基本法としての性格を有し，後半部分（第４章以下）が，民間部門の個人情報保護の一般法としての位置づけを有する 。個人情報保護法（以下，基本法という）１条に書かれている通り，高度情報化社会の進展により，個人情報の適正な取扱いに関する基本理念等を定めることで，「個人情報の有用性 」に配慮しつつ「個人の権利利益を保護する」ことを目的としたものである。前記，判例法上の「プライバシー権（私事をみだりに公開されない権利)」や「自己情報コントロール権」との関係に関してだが，前者では狭すぎ，後者はまだ概念として確立していないことが制定過程で問題とされ ，それら文言を明記しなかった 。もっとも，「個人の権利利益の保護（基本法１条)」の中核部分は判例 のいう「プライバシー権」であり ，その規律は「自己情報コントロール権」の考え方を色濃く反映させたものとなっている 。

2.2.2.保護される「個人情報」「個人データ」「保有個人データ」

本法において保護の対象となっているのは，まず，「個人情報」である。「個人に関する情報 」であることに加え，「生存者性 」「個人識別性」という三つの要件を満たす必要がある（基本法２条)。特に重要なのが「個人識別性」の要件である。氏名，生年月日などの情報がこれを満たすほか，役職名や病歴など特定個人を識別できる情報が広く含まれる。また，他の情報と照合することで個人を識別できるものも規制対象である。このように，個人情報保護法が保護対象としている情報の範囲は極めて広く，身近な情報のほとんどが含まれうる 。

さらに，「個人情報」を含む情報の集合物を，電子計算機等を用いて検索することができるように体系的に構成したもの等を「個人情報データベース（２条５項)」と定義し，これの構成要素となった「個人情報」を「個人データ 」と再定義（基本法２条６項）した上で，「個人データ」はそれに応じた義務（後述）を課すという構造をとっている。個人情報がデジタル情報になると，大量漏洩の危険性が高まるからである 。一方，すべてのデータに関して当該義務を負わせることは酷であることから，「個人情報データベース」の構成要素となった「個人データ」に限定して義務を負うこととした 。

さらに，「個人データ」の中で①「開示，訂正，追加・削除，利用の停止，消去及び第三者への提供の停止」を行うことの許されたもので，②その存否が明らかになることで公益その他の利益が害されるものとして政令で定めるもの又は１年以内の政令で定める期間以内に消去することとなるものを「保有個人データ」とさらに定義しており（基本法２条６項)，それに応じた義務を課している。これは，個人情報取扱事業者（後述）の負担を避けて現実的に実行可能な制度とするとともに，公益等への支障へ配慮したものである とされる。

なお，「個人情報」の部分集合が「個人データ」であり，「個人データ」の部分集合が「保有個人データ」という関係にある （[図１］個人情報等の概念図も参照)。

なお，本事案においても，さらに，先述の Yahoo!BB 事件，TBC 事件においても，漏洩した情報が現行基本法上でいう「個人データ」に該当することには疑いがない。

もっとも，先述の Yahoo!BB 事件では「このような個人情報についても，本人が，自己が欲しない他者にはみだりにこれを開示されたくないと考えることは自然なことであり，そのことへの期待は保護されるべきものであるから」という理由で，プライバシー情報としての保護が肯定された。この事件は，施行前であった個人情報保護法を直接用いることがからこのような表現を使ったのか，また，個人情報保護法の保護から外れうる情報（メールアドレス単体）でも，公開を欲しないことを条件としてプライバシー権としての保護を与える趣旨なのかは不明確である。プライバシー権と個人情報保護法の「個人情報」「個人データ」等を比べると基本的に後者が前者を包含していることは先述したが，細部にまだ整理されていない部分があるのかもしれない。

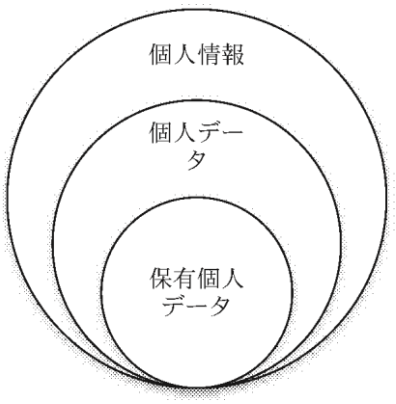

図１ 個人情報等の概念図

2.2.3. 個人情報取扱事業者」が負う義務

基本法は，上記「個人情報データベース」事業の用に供する者を「個人情報取扱事業者」と定義する（２条３項)。この「個人情報取扱事業者 」に基本法４章の各種義務が課されるという構造となっており，それにより個人情報（個人データ）のを保護するという構造である。高度情報通信技術を用いて消費者の消費性向，属性等を含む顧客情報をデータベース化して事業に役立てようとする者を典型例としているとされているが，これも相当広い範囲の主体をカバーする 。Yahoo!BB 事件における Y1 社，Y2 社，TBC 事件におけるＹ社とシステムを受託したＡ社らすべて，現行基本法上でいう「個人情報取扱事業者」に該当する。さて，本件事案においてＸ社もこれに該当することは疑いがない。本件事案は，Ｙ社が不備のあるシステムを供給することにより，Ｘ社に「個人情報保護法違反」をさせてしまった事件というとらえ方ができる。さらに，「外部から個人情報の処理の委託を受けて個人情報データベース等を作成し，委託業者に個人データを提供する情報処理業者も個人情報取扱事業者に該当しうる 」と解されており，本件Ｙ社のように個人情報を預かってシステムを開発する事業者自
体も「個人情報取扱事業者」に含まれる 。

先述の通り，「個人情報」「個人データ」「保有個人データ」という３種類の情報に応じて第４章の義務の規定が使い分けられるという構成となっている。以下，それに応じて簡

単な説明を加えるが，「個人データ」を中心にみるとわかりやすい。まず，「個人情報（個人データ，保有個人データ含む)」に関して課される具体的義務として，まず，取得段階の義務がある。あらかじめ利用目的をできる限り特定し（基本法 15 条），取得の際に当該個人にその目的を通知・公表せねばならない（基本法 18 条)。不正目的による取得は禁止される（基本法 17 条)。次に，当該情報の取扱いも，明示した利用目的（基本法 15 条）の範囲内でのみ行える（16 条)。

次に，「個人データ（保有個人データ含む)」に課される義務として，「データ内容の正確性の確保（基本法 19 条)」が挙げられる。本人の利益をはかる趣旨である 。次に，「安全管理措置（基本法 20 条)」と称して，個人データの漏洩，滅失，毀損の防止などの措置を義務づける。なお，具体的にどのような措置を講ずるかは，分野ごとに各省庁がガイドラインを定める 。後述する通り，本判決ではこのガイドラインが義務づけた（ないし，推奨していた）方法をとらなかった点が債務不履行との関連で問題とされている（後述)。そのほか，「従業者（基本法 21 条)」や「委託先（基本法 22 条)」を監督する義務も課される他，「第三者提供」を制限されており，個人データを第三者に提供するには，本人の同意を得るか，基本法 23 条の規定に該当する事情がなければならない。

最後に，「保有個人データ」に固有の規定として，一定事項を本人の知りうる状態に置く「保有個人データに関する事項の公表等（基本法 24 条)」，本人から開示請求がなされた場合の手続等と，例外的に開示しない場合に関する「開示（基本法 25 条)」，本人から訂正を求められた場合の「訂正（基本法 26 条)」や，基本法 16 条 17 条違反の場合の「利用停止（基本法 27 条)」，また，それらに関する手続（基本法 29 条）などの事項が規定される。

2.2.4. 義務に違反した場合の効果と責任

上記の通り，「個人情報取扱事業者」には，その保有する情報の性質に応じて様々な義務が課され，それに違反した場合には主務大臣から勧告（法的拘束力がない)・命令（基本法違反の場合には勧告を前置しない）（基本法 34 条）がなされるという仕組みになっている。なお，不正な利益を得る目的で個人情報データベース等を提供，盗用した場合には，刑事罰（１年以上の懲役又は 50 万円以下の罰金）も課されうる（基本法 82 条)。

一方，個人情報保護法には，民事責任に関する規定はないため，本法に違反する情報漏洩等がなされた場合には，被害を受けた者は，債務不履行（民法 415 条）や不法行為（民法 709 条）の規定によって個人情報取扱事業者や漏洩の原因を作った者に損害賠償を請求することとなる。

上記の通り基本法に責任の規定が存在しない。個人情報漏洩事件は債務不利履行や不法行為の規定により処理される事となるが，その背後に個人情報保護法の義務が「潜在」していることになる 。

2.2.5. 本件事案との関係

本判決は，個人情報保護法の適用や解釈を大きな問題とはしていないが，あえてシミュレーションするならば以下のように考え得る。まず，Ｘ社もＹ社も「個人データ（Ｘ社の顧客)」を集積した「個人情報データベース」を事業の用に供する「個人情報取扱事業者」であり，基本法 20 条により漏えい防止の義務を負う。しかし，Ｙ社の設計したシステム上の瑕疵を原因として当該個人データが流出し，Ｘ社がその対応をしなければならないことになった。理論的には顧客はＸ社に対して債務不履行責任・不法行為責任を追及することができる。もっとも，Ｘ社が「基本法違反」で顧客から訴え等提起される前に，自主的に顧客へ対応している事案であるため，その点は争点とはなっていない。

３．流出原因の証明

前置きが長くなったが，本判決の検討へ移ろう。まず本件における流出原因が争点とされている。情報セキュリティ技術に通じていない筆者からしても，経産省が当時推奨していた通り，SQL インジェクション（これ自体典型的な不正アクセスの方法である ）に対する脆弱性の対策として，バインド機構の使用とエスケープ処理の対策を設けておくことがある意味「常識」であったことが本判決からうかがえる。これに対して，プログラムの専門家が加わった調停委員会は，SQL インジェクションが流出原因であるとの立証は尽くされていないと述べており（判旨には引用しなかった)，実際に痕跡を残さない形で攻撃がなされていることも指摘されている。にもかかわらず，判決は一般的な不正アクセスの手口（SQL インジェクション攻撃によってデータベースの構造を読み取った後に本格的な攻撃を行う)，Ｘ社が保有していたクレジットカードの不正使用がその時期（４月 14 日－20 日）に増加している点など間接事実から，「14 日までに事前調査としての攻撃」→「14 日から 20 日に本格的な攻撃」→「個人情報の流出」という流れを認定し，その間バインド機構とエスケープ処理が実装されていなかったことが債務不履行（後述）にあたるという認定をなしているが，妥当な結論である。

確かに，専門家から見れば厳密な証明がなされていないと見えるであろうが，そもそもそのような自然科学的な厳密な証明を要求すると，本件のような情報セキュリティ分野の他，医療関係訴訟や保険関係訴訟，環境訴訟など，自然科学的な専門知識が関係する事件のほとんどで一律に責任が認められない事態が生じる 。確かに，専門家の意見は尊重すべきであるが，訴訟における証明は歴史的な証明で足り ，この場面においてもそう考えるべきであろう。

４.債務不履行責任

4.1.契約の性質決定の必要性

本判決において結論を分けたのは債務不履行の部分である。前提問題として，当事者の主張レベルでこの契約が請負契約なのか，委任契約なのかが問題とされている 。本判決の評釈にも同様の争いが見られる。請負契約と考えると，バインド機構等を施していない本件システムは「仕事を完成（民法 632 条)」させる義務に違反していると考えるか否かが問題となる 。委任契約と考えれば，瑕疵のあるシステムを給付したことが善管注意義務違反に当たるか否かが問題とされよう。しかし，データが流出する，個人情報が漏洩するなどにより一律に多数の顧客等が被害を受け，損害額も莫大なものになる情報流出の問題は，制定時の民法が直接想定していない問題であるし，特に本件のような事業者間の問題は約款や契約条項等によって規律されることがほとんどであろう。さしあたり，民法上の契約にあてはめるよりも，個別具体的に契約内容や義務の内容を検討する方が適していると考える 。

4.2. 適切なセキュリティ対策がとられたアプリケーションソフトを提供する義務」とそれへの違反

債務不履行の中身としては，第一に，「適切なセキュリティ対策がとられたアプリケーションを提供する黙示の合意」から「バインド機構の使用・エスケープ処理の施されたプログラムを提供する義務」と合意内容を補充し，それへの違反を債務不履行として責任を認めている。理由として，IPA が紹介するこのセキュリティ対策をなすよう経産省が注意喚起していた点 ，また SQL インジェクション攻撃が多発していた点を挙げている。

この判断のうち「，適切なセキュリティ対策がとられたアプリケーションを提供する黙示の合意」を認定している点には異論はないであろう。顧客情報が流出して差し支えないという意向でシステムの開発・保守を委託・受託する事業者や合意がないことは ，社会通念に照らしても当然のことである。問題となり得るのは，当該「黙示の合意」から「バインド機構の使用・エスケープ処理」の義務を措定したことの当否である。評釈に目を戻すと，当時周知の事実となっていた ，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が所与の前提とされていた ，などと理由づけられている。筆者も，結論として賛成する。現実には，Ｘ社は事業者であるとはいえ，情報セキュリティに詳しくはなかった可能性も高い（だからこそ専門家であるＹ社に委託した）から，経産省の告示等によって契約内容を補充する方法をとることで，結論の妥当性を保ったものと思われる。

ところで，この経産省の告示は，個人情報保護法とどのような関係に立つのか。そもそも個人情報保護法は強行法規である。その個人情報保護法の 20 条は安全管理措置について「個人情報取扱事業者は，その取り扱う個人データの漏えい，滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。」と規定している。しかし，これだけでは不明確すぎ，義務が履行しにくいので，情報セキュリティ分野においては「経済産業分野における個人情報保護ガイドライン（以下，経産省ガイドラインという)」が制定・改正され，逐次最新のセキュリティ対策をするように事業者に求めている。当該ガイドラインの位置づけは「経済産業大臣が法を執行する際の基準」となっており，「本ガイドライン中，「しなければならない」と記載されている規定については，それに従わなかった場合は，経済産業大臣により，法の規定違反と判断され得る。」と書かれている（ガイドラインの改正が複数回行われているが，この点は一貫している)。経産省ガイドラインには，「バインド機構の使用・エスケープ処理」のことは直接は書かれていない。

本判決で引用されている「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」（以下，経産省注意喚起という）は前記経産省ガイドラインとは別に出された告示の一つである。確認すると，個人情報保護法の制定から１年が経過するにもかかわらず個人情報の漏洩が後を絶たないこと，特に SQL インジェクション攻撃が多いことが指摘されており，経産省ガイドラインの「安全管理措置」項目に関して，「その遵守状況を可及的に点検し，遺漏なき漏えい防止対策を確保するよう徹底した取組を行ってください。」と，強い表現で注意喚起をしており，その方法の参考として，IPA ホームページへの参照リンクが設置されており，それをクリックすると「バインド機構の使用・エスケープ処理」の情報が含まれるページへ移る。

厳密に言うと，「バインド機構の使用・エスケープ処理」をしなかったからといって直ちに違法になるわけではなく，「安全管理措置」の方法の一つを経産省が強く推奨しているに過ぎないと解される。もっとも，前述の通り，「安全管理措置」をしないことは違法である。これらはＸ社，Ｙ社それぞれが顧客との関係で遵守せねばならないものであるが，本件で問題とされているＸ社Ｙ社間の契約内容にも「法令や告示を遵守する」「互いに相手に基本法違反をさせない」ことが含まれ，それが債務内容になると考えるべきである。そう考えることで，Ｘ社Ｙ社間に個人情報保護法（特に 20 条）の趣旨や上記告示等の趣旨を読み込むことが可能である。本件Ｙ社は経産省が強く推奨する「バインド機構の使用・エスケープ処理」をするか，しないのであれば，これに匹敵する別の方法で SQL インジェクション攻撃に対する「安全管理措置」をしなければ個人情報保護法違反とされ，そのような事態はＸ社Ｙ社間の契約内容にも反する。

個人情報保護法やそれと同等の効力を有する経産省ガイドラインの趣旨を遵守することは，Ｘ社Ｙ社間の契約内容になっているという考えを推し進めれば，バインド機構の使用・エスケープ処理か，これに匹敵する別の方法を施したプログラムの提供は，「法令を守る」ことと同様，当事者の合意内容に黙示のうちに含まれていたと考えることが可能となる。Ｙ社が提供したものは，当時のセキュリティ水準からいって最低限の質も有していなかった疑いがある。

なお，本研究の主たる論点ではないが，過失相殺についても触れておく。判旨紹介の通り，過失相殺が認められ，Ｘ社３，Ｙ社７という割合で責任を分担する形となっている。本件はＸ社がまず顧客へ謝罪等対応をした額が一応固定化されている（外部関係）ので，残るはＸ社，Ｙ社がどの割合でそれを分担するかの問題となる（内部関係）。Ｙ社が７割の賠償責任を負うことは，現実には情報セキュリティに関するＹ社の専門性が圧倒的に高く，情報漏洩の危険がＹ社の支配下にあったことを表しているように思える。また，判決文 によれば，Ｘ社が「クレジットカード会社名の情報だけを」基幹システムに送信するように指示しており，Ｙ社は「クレジットカード番号」を保存する必要性がないにも関わらず，これを保存する選択をしていることを認定している。本件における情報漏洩に主に責任を負わなければならないのはＹ社であることに異論はなかろう。もっとも，判決文 によれば，Ｘ社にもシステム担当者がおり，判旨のところで紹介した通り，その者が情報保存態様の危険性を認識していたことが認定されている。このＸ社のセキュリティ担当者がどの程度の専門性を持っていたか等不明な点も多く，３割という割合の当否をここで判断することはできないが，Ｘ社側にも責任の一部を負担させた点にも，一定の合理性があったといえよう。

4.3. 暗号化する義務」「説明義務」

ここで，上述の「匹敵する別の方法」として，本件で問題とされているのは「個人情報の暗号化」である。確かに，暗号化された情報は，それに対応した「鍵」がなければ読み取れず，流出したクレジットカード情報等が読み取られなければ，悪用はできない。ところで，本判決は，「暗号化する義務」に関しては，経産省も「望ましい」と述べていたに止まり ，実施すると大きな負担が生ずることを理由として，否定している。この点も検討が必要である。

再度，経産省ガイドラインを参照すると，「「望ましい」と記載されている規定については，それに従わなかった場合でも，法の規定違反と判断されることはない（中略）。しかし，「望ましい」と記載されている規定についても，個人情報は，個人の人格尊重の理念の下に慎重に取り扱われるべきものであることに配慮して適正な取扱いが図られるべきとする法の基本理念（法第３条）を踏まえ，個人情報保護の推進の観点から，できるだけ取り組むことが望まれるものである 」との記載がある。要するに，「望ましい」規定については慎重な取扱いが求められるだけであり，直ちに違法の問題を生じない。債務不履行に置き直して考えると，これを守ることは当然に当事者間の義務となるわけではなく，「特に合意した場合」のみ，それを守る義務が生ずるに過ぎないと考えられよう 。今一度経産省ガイドライン を見ると，「情報の移送・送信時に採用の技術的方法を採用」が「講じることが望まれる手法の例示」として書かれているだけで，さらに，「暗号化して保存せよ」とすら書かれていない。すべての情報を暗号化するとサーバーに負荷をかけるが，一部の暗号化だと暗号化する範囲を特定せねばならない別の負担・費用が生ずる点 も理由となっている。要するに，何か「安全管理措置」をしなければ債務不履行になるが，暗号化の方法は求められていないし現実的ではない一方，経産省が強く推奨し，実施時の負担も軽い「バインド機構の使用・エスケープ処理」が債務の履行方法として最も現実的であり，これをしていなかったＹ社が債務不履行となるという流れである。「個人情報保護法や告示を事業者間契約においても遵守する」という観点から債務内容を検討した場合には，黙示にも暗号化する義務を負っていたとはいえず，その限りにおいて判旨に賛成できる。また，「説明義務」を認定していない点も，何ら不合理ではないと考えられる。説明する以前に，

「バインド機構の使用・エスケープ処理」を施す義務があったからである。もっとも，基本法や告示において遵守すべきラインにとらわれず，情報セキュリティ全般やそれに関連するコンプライアンスの観点からこの事例や類似事例を眺めると，別の結論もありうるかもしれず，今後の議論の展開に注目が必要である。

５.損害に関する判示から推察されること

先述の通り，本判決は，本件流出に関して顧客へ謝罪等の対応が必要になった費用等を中心として，売上損失，システムの再構築など，様々な費目を「損害」として，合計額3231 万 9568 円と見積もった上で，過失相殺（Ｘ側過失３割）をなし，2262 万 3697 円が損害額であるとした。本款では，このうち「個人情報漏洩」により顧客が被った損害に着目してみたい。

上記賠償額（過失相殺前）のうち，顧客への謝罪関係費用が 1863 万 7440 円と主張され，裁判所も顧客への謝罪とその額が合理的であるとして是認しているが，この部分が通常の紛争では，いわゆる「プライバシー権」や「個人情報漏洩」による顧客に生じた損害に相当すると考えられよう。このうち，本件原告の主張によれば，16798 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（被告は「不知」としている)。若干不正確ではあるが，上記情報をもとに顧客（クレジットカード情報の有無を問わず）一人あたりに支払った費用を試算すると，1109.5 円程度となる。なお，仮にクオカードとその包装代（1636 万 2342 円）のみで計算すると，一人あたり 974 円程度となる。

個人情報の漏洩は，漏洩した情報の種類・性質，漏洩の態様や件数など，様々なパラメータにより額が決定されており，単純比較はできないが，一般に 5000 円～50,000 円くらいだと言われている 。参考情報として，まず，顧客からの訴えに対して裁判所が判決で認めた額を確認すると，先述の Yahoo!BB 事件では，一人あたり 6000 円（慰謝料 5000 円，弁護士費用 1000 円)，TBC 事件では，３万 5000 円（慰謝料３万円，弁護士費用 5000 円）であった（うち，TBC 事件では身体等に関わる情報が含まれていた点が高額化に影響した)。本事案は少し低額であることがわかる。

一方，裁判には至っていないが新聞報道等され，企業が「自主的対応」をした事例では，「一人 500 円」の金銭的補償が相場であるようである 。例えば，ベネッセ個人情報漏洩事件 は記憶に新しい。これは，「進研ゼミ」などの教育ビジネスを展開するベネッセの顧客のもとにダイレクトメール（DM）が届くという苦情が頻繁に寄せられ，調査により 2000 万件以上（3500 万件程度）の個人情報（子供と保護者の名前，電話番号，住所等）の漏洩が発覚した事案である。なお，派遣されていたシステムエンジニア（不正競争防止法違反で逮捕されている）が，名簿業者にベネッセの個人情報データベースを数百万円で売って，その後複数の名簿業者を通じて拡散した。ベネッセは，DM を大量郵送するビジネスモデルの刷新，従業員の教育やセキュリティ対策等の措置をとることを記者会見で明らかにしたほか，顧客に対して情報１件あたり 500 円の金券を配布した。しかし，1800 人程度の顧客から，一人あたり５万５千円の損害賠償を求めて提訴されている 。

一方，やや特殊な事例として，プレイステーションネットワーク個人情報漏洩事件 を挙げることができる。これも記憶に新しいが，2011 年に，ソニーの運営するプレイステーションネットワーク（PSN）に登録された顧客 7700 万人分の個人情報（名前，住所，生年月日のほか，クレジットカード番号（ただし，カード番号は暗号化して読み取れないようにしていた)）が流出したと疑われた事件であった。原因はハッカーの攻撃である。ソニーは 2011 年４月 21 日に攻撃に気付き，27 日に情報を公開した。ソニー側は，「おわび」としてゲーム等デジタルコンテンツの無料配布等（時価 3000 円程度のゲームソフト合計 10 本中４本， PlayStation Plus 会員一月（476 円）無料，映画等のオンラインレンタル（400 円～500 円）１本無料，その他）をした。上記の通り，配布したコンテンツ自体は「500 円」の相場からすると相当高額であるが，ユーザーが選べる範囲に制限があり（金券とは違う)，すべてデジタルコンテンツなので「物をおくる」場合と比較して費用は多くかからない他，また，この無料配信が広告につながる側面を持つ（これをきっかけとして有料のコンテンツを購入・利用する客が増える可能性もある）など，やや特殊な事例である。なお，上記サービスをしたのみで，一律の金銭や金券の配布はしていない。なお，ソニーもその後，この情報漏洩の件に関して，海外などで複数の訴訟を提起されている 。

以上のように，裁判例になっている事例では，流出している個人情報の件数も比較的少なく，一人あたりの賠償額は相対的に高くなりがちである。それに対して，新聞報道等なされた大規模な事件では，既に少額の金券を配布しているが，流出した情報は多く，また訴訟まで提起されているものが多いようである。

クレジット番号の変更・取引停止や，DM・勧誘等の電話への対応など，顧客には「500 円の金券」以上の損失が出てい

ることが多いであろう。一方で，裁判より前に１件あたり500 円の金券等を配布するとしても，相当な費用支出へとつながる（仮に１万件として 500 万円，1,000 万件とすると50 億円。それ以外に，本事案でも問題とされたシステム改修費用，調査費用等多額の費用支出も伴う）。このように，個人情報漏洩事件の代表的なものを簡単に比較すると，「訴訟を待たず巨額の支出をして対応をしない訳にはゆかない」ただし，「その対応をしたからといって訴えられるなどして賠償金負担や信用低下が発生するリスクはなくならない」という複雑な状況下に企業が置かれることがわかる。簡単にいうと「板挟み（ジレンマ）」である。具体的には，情報漏洩時に，倫理的には企業は「言われなくとも」すぐにすべての顧客への謝罪やお詫びを形ある方法にて行い，すぐに調査に着手するなど誠意ある対応をとるべきことを顧客も社会も期待している。しかし，現実にその対応はあまりにも巨額な費用を伴うものであるため躊躇することがないとはいえない。そこで，訴訟を提起されるまで待って，和解等をして原告らにだけ賠償金を支払うほうが経済的には合理的かもしれない（情報漏洩を填補する責任保険に入っていれば，保険金が支払われる場合もあり，さらに支出額は軽減される）。しかし，このような対応には筆者は若干の倫理的な抵抗感を覚えるし，対応が後手に回ることでその企業は顧客や市場からの信用を失うであろう。

そのような複雑な「板挟み（ジレンマ）」の状況が存在する前提で，本判決が相当広い範囲（費目）の損害に関してシステム開発者の債務不履行責任を認めたことは，個人情報を保有・管理していた会社（本件ではＸ社）にとって実質的に損害軽減措置の一つとなる。要するに，個人情報を保有していた事業者（漏洩もと企業）は，漏洩が起こったことを察知したらすばやく顧客への謝罪や調査を行って誠意ある対応を行い（外部関係），それにかかった費用をシステムの脆弱性の原因を作ったシステム会社に債務不履行責任の形で分担させる（内部関係）という対応が一部可能となる。本件は事例判断であるとはいえ，「（情報漏洩時）企業に早期の自主的対応を促す」効果も持ちうるように思える。それは，漏洩元企業の信用低下を防ぐ・軽減させる効果も持つと思われ，結果的に損害額を減らす効果もあるだろう。

６. 責任限定の合意

なお，本件事案では，基本契約 29 条２項の責任制限条項の解釈・適用も争われている。本判決は既に紹介した通り，29 条のほうを一般規定，25 条（責任を制限していない）を情報漏洩時の特則と考えた上で，情報漏洩時の責任制限が衡平の観点及び当事者の意思の観点から妥当でないという実質論を展開し，民法の強行規定を参考にしつつ「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」と述べた。さらに，Ｙ社に重過失があったとの認定から，基本契約 29 条２項の条項の適用を排除した。結論として妥当であると考える。情報漏洩による損害（総額）がいくらになるかはその漏洩の態様，漏洩した情報の性質とその件数などによって大幅に変動し，予想することが難しい。加えて，漏洩の態様も従業員の過失による漏洩や持ち出し，外部からのハッキング，システム開発者の過失など，「誰が原因を作ったか」を事前に予測できない。本判決の用いた過失相殺のほうが，事案の実態に即した柔軟な責任分配を可能にする。なお，基本的に自由な内容で契約できる企業間の契約内容を事後的に無効にするための理論構成に，裁判所は若干苦慮したようではある。判決がとった解釈の仕方が若干技巧的に思えるが，実質的妥当性も考慮した上で，本事案限りの判断であると考えれば，理解できなくはない。なお，判決は「重過失」を予見・結果回避が容易であり，故意に近い状態と理解しているが，重過失の意義に関しては紙幅の関係上，ここでは深入りしない 。

実際に情報漏洩が起こった事例の殆どに事業者の過失があり，本件のような重過失が認定されうる事例が多く含まれると考えられるが，そもそも「情報漏洩につき軽過失しかない（重過失がない）」さらに「不可抗力により情報が漏洩する」パターンにはどのような場合があるのか，また，その場合に事業者の責任制限と顧客の損害填補のバランスをどのように考えるか等は，今後の課題である 。さしあたり，筆者は被害者の損害填補やさらなる漏洩防止を重視し，責任が制限される場面は抑制的に考えるのが妥当であると考えており，その点で本判決の結論は妥当であると考える。もっとも，事業者はまず情報漏洩が起こりにくい内部統制システムや情報管理システム等人的側面，情報セキュリティ等の物的側面を充実させ，個人情報が漏洩しないよう，万全な予防策にこそ注力すべきである。さらに，損害軽減策としては，損害賠償費用等の一部を「個人情報漏洩保険」等の保険でカバーする方策を考慮しうるのではないだろうか。

７. おわりに―今後の課題等

以上，本判決を題材としながら，類似の事例との比較，プライバシー権や個人情報保護法との関連などを簡単に検討してきた。おおむね，本判決の判示は妥当であると考える。そもそも，個人情報を取得せずしてビジネスは行えないし，現代のような高度情報化社会においてネットワークやデータベ

ースを構築・利用せねば個人情報の有用性は発揮されない。とはいえ，それら個人情報は常に漏洩の高い危険にさらされており，いったん漏洩してしまうと莫大な費用を個人情報漏洩もと企業等が負担せねばならないのに加えて，訴訟を提起されることでさらなる賠償や信用低下を招く恐れがあることも明らかになった。企業はどの程度膨らむかわからない損害に躊躇しながらも対処しなければならない「板挟み（ジレンマ)」を抱えることも明らかになった。その状況を前提として，先述したように，システム開発者への債務不履行責任を，これだけ多様な費目に渡って認めたことは，漏洩もと企業の自主的対応を（心理的，経済的に）しやすくする効果を持つと思われる。

とはいえ，やはりこのような費用等は高額であることに変わりはない。仮に，これだけの費用を事前予防に利用したらどうだろうか。例えば，従業員教育，個人情報取扱いに関する契約の内容強化と厳しい義務の設定，組織的な情報漏洩防止体制の整備など人的側面のほか，情報漏洩防止のための盤石なセキュリティシステムの構築等物的側面においても，様々な事前予防策を想定できる。情報漏洩時に備えて，情報漏洩保険等に加入しておくことも有益であろう。

本件のような個人情報の漏洩は，従業員のちょっとした出来心やミスなど小さなことや，システムの瑕疵，外部からのハッキングなど予期せぬことから突然起こる。しかし，個人情報の漏洩がひとたび起これば，被害者は数万人から数千万人と多数，被害額も数億から数百億と莫大な額に及びうる。今回は一つのケースに関する研究に止まったが，今後は責任の論点はもちろん，今回検討できなかった内部統制システムなど様々な予防策や保険の問題についても，総合的に検討を加えてみたい。

注

1）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をいい，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 文を実行させるようにして，データベースを攻撃する方法。（滝澤孝臣「判批」私法判例リマークス 51 巻（2015 年（下））31 頁参照。また，やや専門的内容であるが，独立行政法人情報処理推進機構「安全なウェブサイトのつくり方」https://www.ipa.go.jp/security/vuln/websecurity.html（最終アクセス 2016.09. 30）も参照。これにより，当該データベース内の情報を読み取る他，不正操作，破壊，改竄などが可能になる。

2）ソフトウェア及び情報処理システムが 21 世紀の知識経済を支える基盤となることに鑑み，技術・人材の両面から，ソフトウェア及び情報処理システムの健全な発展を支える戦略的なインフラ機能を提供するプロフェッショナル集団として，日本経済の発展に貢献することを目的とする独立行政法人。（独立行政法人情報処理推進機構「IPA について」https://www.ipa.go.jp/about/ipajoho/ gaiyo.html（最終アクセス 2016.09.30）参照。）個人情報を含めた様々な情報漏洩やハッキングを防止するための情報提供と注意喚起，IT 人材の育成や検定試験（情法処理技術者試験）の実施など，情報セキュリティ分野において多方面の活動をしている。

3）予期せぬ SQL を実行しないようにするための対策として，「バインド機構の使用（あらかじめプログラム作成者が想定した SQL 文だけを実行するメカニズム)」」エスケープ処理（SQL において特別な意味を持つ特殊文字を無効化する。)」がある。滝澤・前掲注（1）31 頁，情報処理推進機構・前掲注（1）「作り方」参照。 4）なお，本件仕様変更時にＸが要望したのはカード会社名の情報のみであり，その他の情報はＸの要望の中には直接入っていなかった。

5）Ｘ社は本件ウェブ受注システム委託契約に基づいて支払った代金全額である 2074 万 1175 円の賠償を求めていた。しかし，Ｙ社システム及びＡ社サーバー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する平成 23 年８月 23 日までは，Ｙ社のウェブアプリケーション等の利益を享受していたとしてＸ社の主張を全部は認容しなかったが，Ｘがアプリケーション会社とサーバーを変更したことは，Ｙ社による債務不履行と相当因果関係のある損害であるとした。その額は，平成 23 年２月分から同 24 年１月分の保守サービス・サーバー利用料前払い 63 万円のうち，平成 23 年９月（※この年の８月 23 日まではＹ社を利用していた）から平成 24 年１月までの合計 27 万 5625 円（63 万円×5/12（月）×1.05（消費税５％））が，本文のとおり損害額となる。

6）Ｘ社は個人情報が全件流出したことを前提として，登録顧客全員に見舞金や賠償金を支払うことは必要かつ合理的であると裁判所は認定した。具体的な内訳は以下の通り。①QUO カード及び包装代（1636 万 2342 円），②お詫びの郵送代（124 万 6459 円），③②に関する資材・作業費（封入

や宛名シール貼り等）（86 万 7196 円），④告知郵送代（電子メールで連絡の取れない顧客へ DM 送付；8 万 1440 円），⑤④の郵送代（１万 500 円），⑥お詫びメール配信の外注費（６万 6843 円），⑦お詫び及び QUO カードの書留郵便代（電話，電子メールなどいずれの方法でも連絡の取れない顧客にお詫びの文書と QUO カード送付；2660 円）。

7）本件流出へ対応するために，コールセンター設置を外注し，Ｘ社の従業員を待機させるなどしたため。なお，交通費（深夜対応した場合のタクシー代含む）も含まれる。

8）専門業者２社（ベライゾンビジネス，ラック）に対して本件流出の調査を依頼し，その報告書を作成させた。

9）流出直後の平成 23 年４月 30 日から，同年８月 23 日まで，一時的にラック社のサーバーにシステムを仮移行した費用。

10）サーバー移行により，転職や求人情報に関するウェブサイトであるリクナビネクストの応募フォームを変更する必要が生じ，それを株式会社リクルートに依頼した。

11）平成 23 年４月１日から，同年８月 22 日までインターネット上で，クレジット決済を利用した商品販売ができなかった。その逸失利益としてＸ社は 6041 万 4833 円の損害賠償を請求したが，裁判所は，売上減少を示す決算書が提出されていない点，また，多様な商品が販売されている状況で（支出を免れる）原価を控除する計算がきわめて困難であることを理由として，民事訴訟法 248 条を適用して，400 万円の限度で相当因果関係のある損害と認めた。

12）本判決の判決文（第２ 事案の概要 １ 前提事実（２）基本契約）で問題とされている，Ｘ社Ｙ社間の基本契約（平成 21 年１月 30 日）の契約条項を引用する。なお，契約条項における「甲」が原告Ｘ社，「乙」が被告Ｙ社である。

（引用はじめ）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）

（引用終わり）

13)殆どの情報は現在電子化され，ネットワークを通してやり取りされている（企業に限られない)。それに対する不正アクセスが高度化，巧妙化している現在，「善意のハッカー（ホワイトハッカー)」すなわち，サイバー攻撃を防衛するための専門家を育成する取組みがなされつつあるが，人材不足が深刻である（『日経新聞（電子版)』 2015年６月７日「ウイルス作り敵を知る 正義のハッカー育成」，同2016年１月18日「「善意のハッカー」育成サイバー攻撃から企業守る」)。

政府等の国家機関が攻撃されることをまず防がなければならず，すでに政府は「ホワイトハッカー」を採用している（『日経新聞（電子版)』2015年２月21日「政府，ホワイトハッカー25人前後採用 15年度」)。他に，発電所や工場などがサイバー攻撃を受けた場合に非常に重大な社会的影響を及ぼすことなどから，経産省はサイバー防衛人材の訓練所を設立する計画を立てている（『日経新聞（朝刊)』2016年８月10日「サイバー防衛の人材育成拠点 経産省，インフラ向け」，『日経新聞（電子版)』2016 年７月５日「工場・発電所をサイバー防衛 産学官が相次ぎ対策」)。このような人材育成は，個人情報・営業秘密等企業情報の漏洩防止にとっても急務であろう。

14)判時2221号71頁掲載。なお，評釈として遠藤元一「判批」横浜法学24巻２・３号191頁（2016年)，滝澤・前掲注(１)30頁（2015年)，上山浩「判批」NBL1055号34頁

（2015年)。

15)Yahoo!BB事件に関する評釈として，神作裕之「判批」廣瀬久和・河上正二編『消費者法判例百選（別冊ジュリ 200号)』236頁（有斐閣・2010年)，田中宏「判批」リマークス36号（2007年上）67頁（2007年)。

16)高橋郁夫「コンピュータ委員会報告’04「個人情報漏洩事件とその対策」報告」日弁連法務研究財団ホームページ（https://www.jlf.or.jp/jlfnews/vol25_5.shtml（最終アクセス2016.09.30)）参照。

17)TBC事件に関する評釈として，浦川道太郎「判批」リマークス38号（2009年（下））66頁。

18)判タ165号184頁掲載。評釈として，根森健「判批」長谷部恭男ほか編『憲法判例百選①（第６版)』138頁（有斐閣，2013年)，伊藤正己「判批」小林直樹編著『ジュリスト増刊 憲法の判例（第３版)』125頁（有斐閣，1977年)。五十嵐清「判批」伊藤正己編『マスコミ判例百選（第

２版)』122頁（有斐閣，1971年)。

19)本文で紹介した「宇治市住民票データ漏えい事件」以外の判例で，「プライバシー権」に関係があるものとして，いわゆる「前科照会事件（最高裁昭和56年４月14日民集35巻３号620頁)」を挙げることができる。これは，弁護士法23条の２に基づく照会に対して，自治体が当該市民に関する犯罪歴等を照会してしまい，当該情報を公開された市民が国家賠償法１条に基づいて損害賠償を求めた事案であり，最高裁は賠償責任を認めた。前科及び犯罪経歴をみだりに公開されないという法律上の保護に値する利益があり，みだりに当該情報を漏洩してはならないという判示は「プライバシーとしての重要性を考慮して，前科に関する情報を保管する官庁にその管理について高度の注意義務を課し」たものである（判タ442号56頁（判決コメント)）。

20)判時265号11頁。なお，評釈として，齋藤義浩「判批」法時78巻８号92頁（2006年)，右崎正博「判批」『ジュリ臨増 平成13年度重要判例解説』８頁（有斐閣，2002年)，徳本広孝「判批」磯部力ほか編『地方自治判例百選（第４版)』37頁（有斐閣，2013年)，藤原静雄「判批」赤尾太郎ほか編『サイバー法判例解説（別冊NBL79号)』190 頁（商事法務研究会，2003年)。

21)芦部信喜著・高橋和之補訂『憲法（第６版)』123頁（岩波書店，2015年）は，公権力対私人という文脈であるが，「自己に関する情報をコントロールする権利（情報プライバシー権)」というとらえ方により「プライバシーの保護を公権力に対して積極的に請求していく側面が重視されるようになってきている」と述べる。

22)評釈として山崎友也「判批」『ジュリ臨増1376号 平成20年度重要判例解説』11頁（有斐閣，2009年)，山本龍彦

「判批」『憲法判例百選１（第６版)（別冊ジュリ217号)』 46頁（有斐閣，2013年)，高橋信行「判批」『地方自治判例百選（第４版)（別冊ジュリ215号)』36頁（有斐閣，2013 年）など参照。

23)芦部・高橋・前掲注(21)124頁は「情報プライバシー権的考え方を示唆するもの」として，この最判平成20年住基ネット最高裁判決を紹介している。もっとも，判決のコメント（判タ1268号111頁）は「「自己情報コントロール権」が憲法上の人権であるか否かについて判断を示すまでもないと解したものと考えられる」としている。学説にお

ける「自己情報コントロール権」の考え方を判例法理に位置づけることに最高裁は慎重であることがうかがえる。

この事件において最高裁は，住基ネットの本人確認情報などが必ずしも秘匿性が高いとはいえないものであること，漏洩の具体的危険は発生していないことなどを理由として，憲法13条の上記権利を侵害するものではないとして，合憲の判断をしている。

なお，「自己情報コントール権」に関する裁判として，芦部・高橋・前掲注(21)124頁では「江沢民講演会参加者名簿提出事件（最判平成15年９月12日民集57巻８号973 頁)」を挙げている。講演会に参加した者の名簿を，警察の要請に応じて大学が警察に提出した事案において，「本人が，自己が欲しない他者にはみだりにこれを開示されたくないと考えることは自然なこと」であり，当該個人情報が「プライバシーに係る情報として法的保護の対象となる」と判示する部分がそれである。

その他，下級審判決ではあるが，マンション会社が管理会社に顧客の勤務先情報を無断提供し，当該顧客のもとに管理会社から電話をかけられた点などから当該顧客がプライバシーの侵害を理由にマンション会社を訴えた事件がある。判決（東京地裁平成２年８月29日判時1382 号）が「プライバシーの権利は，このように，自己に関連する情報の伝播を，一定限度にコントロールすることも保障することをその基本的属性とするものと解される」として，勤務先名称と勤務先電話番号がプライバシー権による保護をうけることを明らかにし，その内容を「自己情報コントロール権」として捉えている（ただし，緊急時の連絡のための開示でもあった点，不動産購入者全員が管理会社への開示を承諾していた点などから，正当理由があったとして，不法行為責任は結論として否定した)。

24)この法律に関する文献として，右崎正博ほか編『別冊法セミ224号 新基本法コンメンタール 情報公開法・個人情報保護法・公文書管理法（情報関連７法)』164頁以下（日本評論社，2013年)，宇賀克也著『個人情報保護法の逐条解説（第４版)』(有斐閣，2013年）など。なお，最新の平成27年改正の内容を盛り込んだものとして，瓜生和久編著『一問一答 平成27年改正個人情報保護法』(商事法務，2015年)。なお，本法制定の経緯の詳細な記述として，赤堀勝彦著『企業の法的リスクマネジメント』55頁以下（第２章）（法律文化社，2010年)。

25)赤堀・前掲注(24)59〜60頁。

26)赤堀・前掲注(24)55頁。

27)制定後，これまでの間に情報通信技術の発達により多種多様なパーソナルデータが「ビッグデータ」として活用される状況が生まれた。そこで，平成27年改正においては，パーソナルデータの円滑な利活用を促進させ，新産業・新サービスの創出を実現するための環境整備をするために個人情報保護法を見直し，１条に「新たな産業の創出」「活力ある経済社会及び豊かな国民生活の実現」などの具体例も挙げられた（瓜生・前掲注(24)３頁・９頁)。

28)衆議院「個人情報の保護に関する特別委員会の会議録議事情報一覧」(http://www.shugiin.go.jp/internet/itdbkaigiroku.nsf/html/kaigiroku/0130_l.htm（最終アクセス2016.09.30)）第２号（平15・４・14)，第３号（平15・４・15）参照。

29)自己情報コントロール権侵害への救済として，情報の開示請求や訂正・削除の請求などをするには基本法の存在を前提とする（曽我部真裕ほか著『情報法概説』176頁（弘文堂，2016年))。これら請求権に関しては，基本法が「自己情報コントロール権」を具体化したものと考えても差し支えない。

もっとも，損害賠償に関しては，流出した個人情報がプライバシー情報等にも該当する場合は，漏洩もと事業者などは二重の責任を負いうるとの説（岡村久道「個人情報保護法と企業の対応―損害保険分野を例として」予防時報216号43頁参照）もある。「個人情報保護法」違反がすなわち「自己情報コントロール権」の侵害なのか，という問題に関してはまだ未解明の部分が残っている。

30)最判平成15年９月12日民集57巻８号973頁参照。

31)右崎ほか・前掲注(24)171頁，175頁（小町谷育子＝三宅弘執筆)。

32)右崎編・前掲注(24)171頁（小町谷育子＝三宅弘執筆）参照。

33)個人を保護する法律（基本法１条）なのであるから，法人の情報や，法人の機関としての個人の情報は原則として保護されないが，役員や機関を離れた純粋に個人としての情報は保護される（右崎ほか・前掲注(24)173頁（小町谷育子＝三宅弘執筆))。

34)死者は開示請求ができないこと，遺族等の第三者の保護を目的としていないことなどが主たる理由であるが，死後症例の分析等に用いる必要があるとの日本医師会の指摘も大きな根拠となった（右崎ほか・前掲注(24)174頁（小町谷育子＝三宅弘執筆))。なお，死者の情報と遺族の情報が

密接不可分の関係にあれば，遺族の情報として保護されうる（同）。

35) なお，平成 27 年の改正において，前述の「個人を識別することのできる情報」に新たに「個人識別符号（改正基本法２条２項）」が含まれるようになった。この「個人識別符合」は，①身体の一部の特徴をデータ化した文字，番号，記号その他の付合や，②サービスの利用者や個人に発行される書類等に割り当てられた文字，番号，記号，その他の符号のうち政令で定めるもの，のいずれかに該当するものが含まれる（瓜生・前掲注(24)10－11 頁）。指紋や顔の特徴をコンピュータ処理したもの，マイナンバー，旅券・運転免許証番号，基礎年金番号などがこれに該当する（同・14 頁）。

36) 現に」個人情報データベースを構成することは要件ではないので，個人データが出力されたハードコピーや，マニュアル処理の個人情報データベース等のコピーも「個人データ」に該当する（宇賀・前掲注(24)「逐条解説」38 頁）。また，病院のカルテなど，コンピュータを用いる場合に匹敵する検索が可能なマニュアル情報は「体系的に構成したもの」の文言に該当し，含まれる。

一方で，インターネットの検索エンジン（特定個人の検索を想定していない），カーナビに入った情報（電話番号や住所，法人や公共施設名のみで，個人名は含まない）ものは「個人情報データベース等」に該当しない（右崎編・前掲注(24)178 頁（小町谷育子＝三宅弘執筆）参照）。

37) 宇賀・前掲注(24)「逐条解説」38 頁。

38) 宇賀・前掲注(24)「逐条解説」38 頁。

39) 宇賀・前掲注(24)「逐条解説」39 頁。

40) 宇賀・前掲注(24)「逐条解説」39 頁。

41) なお，基本法２条３項各号の団体等が除かれる（別の法律による規律）ほか，「データベースを事業の用に」供していない場合（個人の年賀状ソフトなど），などは「個人情報取扱事業者」から除かれる（右崎ほか・前掲注（24）178 頁（小町谷育子＝三宅弘執筆））。なお「小規模事業者」に該当する場合（取扱個人情報 5000 件以下の場合）の適用除外規定が存在した（平成 27 年改正前基本法２条３項５号）が，インターネットを通じて情報が瞬時に拡散する危険性等を理由として，平成 27 年改正において廃止された（つまり，5000 件以上か以下かに関係なく適用を受ける）。

42) 右崎ほか・前掲注(24)178 頁（小町谷育子＝三宅弘執筆）。

43) ポジティブリスト方式を採用しなかったのは，漏洩の危険を考慮してのことである。その団体の内容・規模を問わず，営利・非営利を問わない（右崎ほか・前掲注(24)178－179 頁（小町谷育子＝三宅弘執筆））。

44) 宇賀・前掲注(24)『逐条解説』31 頁。

45) 仮に顧客が訴えを提起した場合には，個人情報保護法 20 条違反を理由に，Ｙ社を被告として直接不法行為責任を追及することが理論的に可能である。もっとも，実際に顧客にはシステムに関する専門知識がなく，Ｙ社が漏洩の主たる原因を作ったことまで知ることは期待できないため，原告たる顧客は，Ｘ社を被告とするか，Ｘ社とＹ社の両方を被告とする方法が現実的である。本稿が「外部関係」と呼ぶ紛争の殆どはこのような類型である。

46) 右崎ほか・前掲注(24)206 頁（新保史生執筆）。

47) 右崎ほか・前掲注(24)208 頁（新保史生執筆）。

48) 債務不履行構成によれば，情報を取得する際の合意・契約などに「個人情報保護法を守る」点が明示・黙示に含まれる等と考えるなど，また不法行為の場合には，「個人情報」を被侵害利益と考える，基本法違反を「違法性」要件の中で考慮するなど，少し工夫が必要であると思われる。なお，先述の通り，基本法の保護する「個人情報」と判例法上の「プライバシー権」は密接な関係にあるものの別のものであるので，理論上はそれぞれについて損害賠償請求をすることが可能となる。

49) 上山・前掲注(14)36 頁。

50) 上山・前掲注(14)37 頁参照。

51) 最判昭和 50 年 10 月 24 日民集 29 巻９号 1417 頁（ルンバール事件）参照。通常陣の確信を基準として，事実に関する高度の蓋然性が証拠によって基礎づけられることが必要で，それで足りる（伊藤眞『民事訴訟法［第４版補訂版］』332 頁（有斐閣，2014 年））。なお，ルンバール事件はルンバールと呼ばれる施術（頸椎に針を刺して髄液を採取する）を行ったことで運動障害等の後遺症が残った事例であったが，この因果関係が科学的に証明されていなくとも，他に「特段の事情が認められない限り」経験則上因果関係を認めるのが相当であるとした（因果関係の一応の推定）。

52) Ｙ社が請負契約と主張している。そう解すると，本件基本契約 26 条２項が適用され，責任期間が１年となり，金種指定詳細化の時点ではすでにその期間が満了していたという主張である。

53) Ｘ社がＹ社に本件システムの設計，保守等を委託し，Ｙ社がその仕事の完成義務を負っていた点から請負契約と解

する立場（遠藤・前掲注(14)203 頁）がある。本件は瑕疵担保責任として論ずるべきであったという観点から本件契約を請負契約と解しているようだが，検討の結果，結論として債務不履行構成をとっても，瑕疵担保責任構成をとっても決定的な相違はないと結論づける（同 205 頁）。

54)なお，Ｘ社のようなユーザーとＹ社のようなベンダーの関係が委任契約から請負契約へと段階的に進展していき，それに伴った法的拘束力を観念し得るとする立場があり，同立場は一般的にこのような契約はユーザーの協力が不可欠であることに着目し，ベンダーに「プロジェクト・マネージメント義務」，ユーザーに「協力義務」が課されると解する（滝澤・前掲注(１)33 頁。なお，滝澤孝臣「判批」リマークス 47 号 18 頁以下，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」 NBL1050 号４頁以下等も参照)。確かに，本件のような契約は企業のみならず官公署，大学などの研究教育機関など，様々な団体が用いる契約類型であり，それらに共通する要素を検討してみる価値は高いと考えられ，今後の検討課題としたい。

55)経産省ホームページ（経産省「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（平成 18 年２月 20 日付)」http://www.meti.go.jp/policy/it policy/privacy/kanki.html（最終アクセス 2016.09.30)）によれば，「公開すべきではない情報の「非公開ファイル」としての区分保管」「ソフトウェアの維持に必要な修正プログラムの適切な適用」「推測可能なパスワードの排除」「ファイル等へのアクセス制限措置の導入」「ファイアウォールの設置」「セキュリティ監査の定期的実施」などの項目について，「重点的に点検及び漏えい防止対策を実施してください」と記されており，情報処理推進機構のホームページ（同「脆弱性関連情報の取扱い：ウェブサイトのセキュリティ対策の再確認を～脆弱性対策のチェックポイント～」（http://www.ipa.go.jp/security/ vuln/20050623 websecurity.html（最終アクセス 2016.09. 30)），同「安全なウェブサイトの作り方」(http://www.ipa.go.jp/security/vuln/20060131_websecurity.htm（l 最終アクセス 2016.09.30))）を参照するようにとの指示書きがある。

56)滝澤・前掲注(１)33 頁。

57)上山・前掲注(14)38 頁。

58)遠藤・前掲注(14)212 頁。

59)経産省・前掲注(55)。

60)判時 2221 号 86 頁参照。

61)判時 2221 号 87 頁参照。

62)経産省のガイドライン（平成 19 年３月 30 日付 経産省告示第１号「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」（http://search. e-gov.go.jp/servlet/Public?ANKEN_TYPE＝3&CLASS NAME＝Pcm1090&KID＝595106051&OBJCD＝& GROUP（最終アクセス 2016.09.30))）は，「①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の実施」という項目で，クレジットカード情報の「保存期間の設定・保存場所の限定」「情報の移送・送信時に採用の技術的方法を採用」など６項目の措置を推奨しているにとどまる。

63)経産省・前掲注(60)「個人情報保護ガイドライン」１頁参照。

64)滝澤・前掲注(１)33 頁参照。

65)経産省・前掲注(60)「個人情報保護ガイドライン」61 頁。

66)遠藤・前掲注(14)212 頁，上山・前掲注(14)39 頁。

67)牧野和夫「個人情報漏えい事件と具体的企業対応」会社法務 A2Z・2014 年 11 月号 16 頁。なお，この文献には本文で紹介したような事件を，裁判を経た事例と自主対応（まだ判決前）の事例とに分け，事案の概要，流出した情報，その損害額や謝罪費用等を比較しており，参考になる。

68)『日経新聞（電子版)』2014 年７月 20 日「顧客情報漏洩，過去の補償「１人 500 円」めだつ」参照。

69)『日経新聞（電子版)』2014 年７月 16 日「派遣 SE「データ数百万円で売った」ベネッセ漏洩」，同 2014 年９月 11 日「ベネッセ漏洩 3504 万件に DM 営業，徹底見直し」，など参照。 70)『日経新聞（電子版)』2015 年１月 30 日「ベネッセ漏洩で 1789 人が提訴」

71)『日経新聞（電子版)』2011 年４月 27 日「ソニー情報流出 侵入手口の二つの可能性」，株式会社ソニー「PlayStation Network/Qriocity™をご利用の皆様へのお詫びとお願い」(http://cdn.jp.playstation.com/msg/ sp 20110427_psn.html（最終アクセス 2016.09.30)），同「感謝とおわびのパッケージ」(http://cdn.jp.playstation.com/psnmsg/package.html（最終アクセス 2016.09.30)）参照。

72)『日本経済新聞（電子版)』2011 年４月 28 日「米男性がソニー提訴 個人情報の大量流出で」参照。

73)例えば，加藤一郎『不法行為［増補版]』75 頁（有斐閣・ 1974 年）は，重過失を「著しく注意を欠いた場合」であると捉え，故意と過失には質的差異があるが，軽過失と重過失は，質的には差異がなく，単に量的差異があるに過ぎないと捉える。同・75 頁によれば，「故意と過失の中間でかなり軽いものまで入るという考え方」もあり，「故意に準ずるものというほど厳格に解することもないと思われる」。他に，幾世通著・笹本伸一補訂『不法行為法』 45

頁，184〜185 頁（有斐閣・1993 年）参照。学説における重過失のとらえ方自体は多様である。なお，これら文献は民法と「失火責任法」における「重過失」について一般論を述べた文献である。ネットワークを通して大量の情報が漏洩し，瞬時に莫大な損害が生じる個人情報漏洩事件における「重過失」は別異に解する余地があるかもしれない。

74) なお，顧客との間でこのような責任制限条項を結んだとしても，消費者契約法８条の「責任を免除する条項」に関する問題となるであろうが，全部免除する条項は８条１項１号により無効になると考える。また，「情報漏洩による責任を〇×△に限る」旨の条項は８条１項２号の一部免除条項の問題になり，当該漏洩に関する過失の有無が問われると考える。