SOFTIC判例ゼミ 2024（第3回）

MENET事件

前橋地裁令和5年2月17日（令2ワ145号）

2024年10月18日

土方 伊藤

目次

1. 事案概要
2. 争点一覧
3. 関連裁判例
4. 情報セキュリティ・サイバーセキュリティ関連参考資料
5. ディスカッションポイント

1. 事案概要

1．当事者

原告：前橋市
被告：東日本電信電話株式会社（NTT東日本）

2．事案概要

2015年5月21日　前橋市情報教育ネットワーク（**MENET**）のデータセンター移管設計及び構築業務（**本件システム**）に係る**委託契約を締結**（契約金額:1億480万500円）*
2015年9月30日　本件システム(完成図書含む)の**引渡し/検収完了****
2015年10月1日　データセンターの移管保守業務に係る保守契約を締結（月額100万円）
2018年3月16日　MENETヘルプデスク担当者が、**教育資料公開サーバに対する不審なアクセスログを確認**。2017年8月頃、何者かが本件システムの教育資料公開サーバーにバックドアを設置し、12月中旬頃には、内部ネットワーク内へ侵入を行っていた。（**本件不正アクセス**）
2018年3月30日　本件不正アクセス調査の結果、3月6日に攻撃者が教育資料公開サーバーに個人情報ネットワークサーバーに保管される多数の個人情報を圧縮して収集・保存を行い、当該情報へのアクセスが多数確認され、**多数の個人情報（児童生徒ら約4万7,000人分）が流出した可能性が高いことが判明*****
2018年6月20日　原告の依頼により本件不正アクセスの「検証報告書」が作成される
2019年1月28日　原告が損害賠償請求　約1.8億円（交渉決裂）
2020年3月26日　原告が提訴
2023年2月17日　前橋地裁判決　**原告勝訴**。被告控訴、原告附帯控訴
2024年2月28日　東京高裁判決言渡し予定も**裁判所判断で延期**
2024年12月11日　東京高裁判決言渡し予定

2．事案概要（続き）

***MENETの概要**

1998年：市内の小中学校や教育機関を結ぶ情報通信ネットワークとして運用を開始する
市教委内の技術者が主導となり、民間ボランティアが協力して発展する
2005年頃：校務支援システムを導入し、個人情報を取扱い始める
2010年：総合教育プラザ内にNOCを設けて運用され、市の行政ネットワークとも接続され、
資産評価や学校評価のシステム等が追加され、さらに学校給食管理システムも導入される
2012年：教育資料をデータ化して検索可能な教育資料検索システムが導入され、教育資料公開サーバを
通じて公開された

市教委内の異なる組織により、それぞれが所掌するサーバが置かれるようになった。

本件システムの委託契約の概要

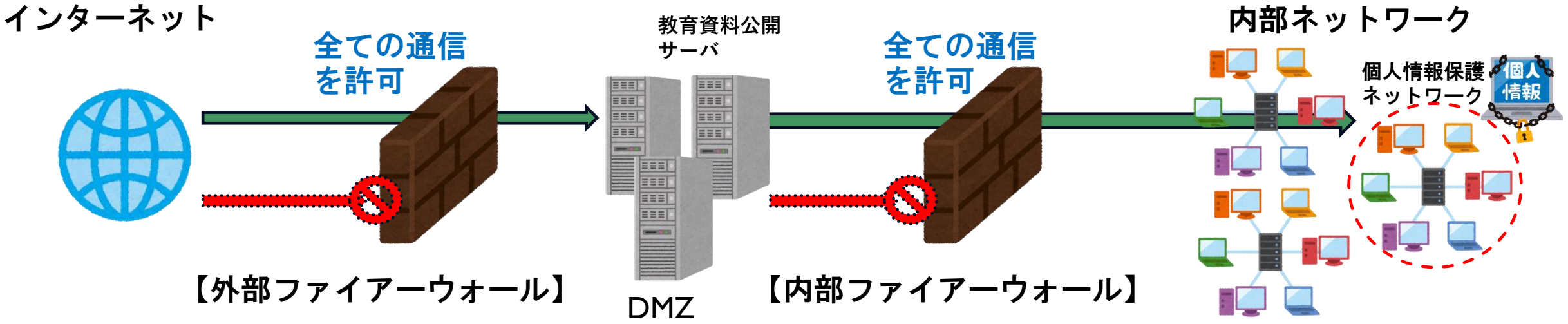
ＭＥＮＥＴの設備更新時期を迎え、安定したサービス提供や効率的・機能的なシステム構築を目指し、
総合教育プラザ内に設置されたすべてのネットワーク機器やサーバ等をデータセンターへの移管・構築
（「検証報告書」より）

2．事案概要（続き）

本件システム納品時のファイアウォール設定状態

・**ファイアーウォール**：主な機能として送信元/送信先（IPアドレス・ポート）を設定し、許可された通信のみを通し、許可されていない通信を遮断する機能（フィルタリング機能）

・**DMZネットワーク**　：緩衝地帯のネットワーク。
セキュリティを高めるために外部ネットワークと社内ネットワークの間に設置。



本件システム納品時には、いずれのファイアーウォールも**全ての通信を許可する設定**となっており、インターネットを通じて外部からDMZを経由して内部ネットワークへ容易にアクセスが可能な状況であった。

２．事案概要（続き）

*****流出した可能性がある個人情報の内容**

平成24年（2012年）度から平成29年（2017年）度までに、前橋市の公立小・中学校及び特別支援学校に在籍した**全児童生徒の給食費に関する４万７８３９人のデータ**（学年、組、出席番号、氏名、性別、生年月日、国籍、住所、電話番号、保護者氏名、アレルギー、既往症等）や、同時期に市立学校（園）で給食を喫食していた**園児児童生徒及び教職員の給食費の引落口座情報２万８２０９件**（銀行名、支店名、口座番号、預金者名、引落金額、振替結果）

（「検証報告書」より）

請求の趣旨

本訴：被告は、本件システムのファイアウォールを適切に設定することにより通信制限を行う債務・注意義務があったにもかかわらず、これを怠り、本件不正アクセスを発生させ、原告に損害を負わせたとして、**債務不履行／不法行為による損害賠償請求**を求めた。
請求金額は1億7,735万6,440円。

反訴：被告は、原告から委託されたMENETサーバのデジタルフォレンジックやHDのクレンジング作業等に要した費用等の**償還請求**を求めた。
請求金額は1,159万3,184円

判決

本訴：被告は、原告に対し、**1億4,298万444円を支払え。**
反訴：原告は、被告に対し、952万2073円を支払え。
訴訟費用負担：本訴では、原告：被告で18:82、反訴では、原告:被告で82:18

2．争点一覧

本訴の争点

① 委託契約に基づく外部ファイアウォール及び内部ファイアウォールを適切に設定することにより通信制限を行うべき債務の不履行又は注意義務違反（不法行為）の有無（争点①－１）

② 保守契約に基づく外部ファイアウォール及び内部ファイアウォールの設定における通信制限の不備を修正すべき債務の不履行又は注意義務違反/不法行為の有無

③ 想定されるリスク及びその対策について適切な提案をすべき注意義務違反/不法行為の有無

④ 債務不履行又は不法行為と本件不正アクセスとの間の相当因果関係の有無

⑤ 原告の損害　（争点②）

⑥ 被告の債務不履行に係る帰責事由の不存在（抗弁）（争点①－２）

⑦ 責任限定契約の適用の有無（抗弁）（争点③）

（ご参考）反訴の争点

・準委任契約に基づく費用等の償還請求
・商法５１２条の規定に基づく報酬請求権

争点①－１　委託契約に基づき外部ファイアウォール及び内部ファイアウォールを適切に設定することにより通信制限を行うべき債務の不履行又は注意義務の有無

【原告の主張】

委託契約では、提案依頼書から基本契約書に至るまで一貫してセキュリティ対策が重要視されているのであるから、被告は、同契約において、個人情報保護ネットワークに保存されている個人情報を保護するため、**本件システムの提供に当たり、その外部ファイアウォール及び内部ファイアウォールを適切に設定して通信制限を行う債務を負っていた。**

【被告の主張】

原告が主張するような債務が契約書に明示されているわけではなく、**適切に設定することによる通信制限を行う義務のような観念的抽象的な債務を負うものではない。**

【裁判所】

委託契約において受託者である被告が負う債務の内容は、同契約の契約書の記載の内容のみならず、**同契約の前後にやり取りがされた要件定義書や基本設計書などの内容を総合的に考慮して確定すべきである**と解する。

①提案依頼書、提案書、要件定義書及び基本設計書には、外部ファイアウォール及び内部ファイアウォールにより通信制限を行う旨の記載があること

②設計方針及び基本設計書には、データセンター内理論接続図及び通信制限イメージにおいて、ＤＭＺネットワークと個人情報保護ネットワークとをつなぐ通信経路が存在しないこと

③被告は、経験豊富な専門家を多数擁する技術的セキュリティ対策チームによる総合的なセキュリティソリューションを提供することを可能とする技術力を有していたこと

①～③の認定に基づき、被告は、委託契約において、ＤＭＺネットワークと個人情報保護ネットワークとの間の通信経路を遮断するため、本件システムの提供に当たり、**その外部ファイアウォール及び内部ファイアウォールを適切に設定して通信制限を行う債務を負っていた。**

争点①ー２　被告の債務不履行に係る帰責事由の不存在（抗弁）

【被告の主張】

・納品した完成図書には、外部ファイアーウォール及び内部ファイアーウォールについて実際にされた設定が記載されており、原告はその設定について了解ないし認識していた。

・委託契約に基づき原告は検査をする義務があり、原告は上記の記載について了解ないし認識のもと完成図書を検収していた。

【裁判所】

・本件システムの完成図書は、大部であり、かつ、コンピュータ言語で記載されていることが認められ、その交付を受けた者がその全体を見て本件システムが自らの要求を満たすものであるか否かを確認することは現実的に困難であり、不可能に等しいものというべき。

・①提案依頼書、提案書、要件定義書及び基本設計書には、外部ファイアウォール及び内部ファイアウォールにより通信制限を行う旨の記載がある
②設計方針及び基本設計書には、データセンター内理論接続図及び通信制限イメージにおいて、ＤＭＺネットワークと個人情報保護ネットワークとをつなぐ通信経路が存在しないこと
これら事実に照らせば、**外部ファイアーウォール及び内部ファイアーウォールが不適切な設定になっていることは想定し難い事実**であったといえる。

・原告と被告との間のコンピュータシステムの構築などの専門性には相当の格差があることは、**当裁判所に顕著な事実**である。

・被告が原告に対して本件システムを引き渡した時点において、**原告に対してファイアウォールの不適切な設定について告知ないし説明をしていたというのであれば格別**、そうでない以上、**被告に責めに帰すべき事由がないということはできない**というべき。

争点②　原告の損害

【裁判所の損害認定にあたり依拠した基準】

以下の２資料を参照し、被告の債務不履行を原因とする本件不正アクセスとの関係で相当因果関係のある通常生ずべき損害（通常損害）と認められるか否か（弁護士費用は除く）

【基準１】「サイバーセキュリティ法務」（商事法務）より

①インシデント情報の**検知**
②インシデント情報の**分析**（トリアージ）
③**初動対応及び証拠保全**
④**当局対応及び情報開示**
⑤原因分析及び再発防止
⑥**事後対応**（被害者への補償、被害回復及び責任追及）

【基準２】Gが作成した「情報セキュリティセミナーインシデントマネジメント(v1.0)」より

①組織体内部のコミュニケーションや関連組織とのコミュニケーション
②**暫定的対応として、ネットワーク接続の切断、サービスの停止など**を行うこと
③**本格的対応**として、攻撃者にシステム特権を奪われてしまったときは、悪意あるプログラムを仕掛けられていないことを検出し、それが存在しないことを保証することは不可能に近く困難であることから、**原則としてクリーンなシステムを再構築する必要があり、信頼できるメディアからクリーンなシステムを再インストールし、修正プログラムを適用した上で、設定ファイルの情報やデータをバックアップから復旧する**こと
④改善を図ること

争点②　原告の損害

【裁判所が認めた項目一覧①】

損害項目	理由
１．デジタルフォレンジック対応業務委託料(918万円)	基準１の②及び③の観点から、本件不正アクセスが検知された後の対応として必要かつ相当な範囲内の損害である。
２．インシデント対応支援コンサルティング業務委託料(540万円)	基準１の③及び④に関する業務といえ、本件システムの規模や本件不正アクセスの内容に照らし、原告において専門的知識や経験を前提としたコンサルティング要務を依頼することも合理的であり通常損害である。
３．保護者・教職員宛通知の郵送料等(370万0766円)	本件不正アクセスにより、児童、保護者、教職員ら多数の個人情報が流出した可能性が高いことが判明したことに照らし、基準１の④及び⑥に関する対応として、彼らに通知を発し、その経緯の説明や注意喚起を図ることは必要かつ相当のであり、これらに要した費用は通常損害である。
４．職員時間外勤務手当処分等(455万8066円)	本件不正アクセスを受けた対応として、コールセンターを設置し、通知文書の発送をすることは、基準１の④の観点より、必要かつ相当なものであり、職員の時間外労働手当分及び週休日休日の振替等により低下した労働力分は通常損害である。

争点②　原告の損害

【裁判所が認めた項目一覧②】

損害項目	理由
５．第三者委員会委員報酬当等(112万8560円)	流出した可能性がある個人情報がセンシティブな内容を含むものであり、規模も大規模なものということができ、基準１の②、④及び⑤に関し第三者的な視点から慎重に行うことは合理的であり、これら作業が専門的知見を要するものであることも踏まえると、第三者委員会を設置して事実確認を行ったことは合理的な措置といえ、通常損害である。
６．各種外部ネットワーク調査業務(Web調査)委託料(1107万円)	流出した可能性がある個人情報がセンシティブな内容を含むものであり、規模も大規模なものということができ、基準１の②及び④の観点から、流出した可能性のある情報がインターネット上に存在するか否かを調査する必要性は高いといえ、その調査の性質上、専門的な知見を有する者に対して委託することも合理的であり、通常損害である。
７．MENET校務系末端復旧作業業務委託料(3242万5380円)	基準２の③の観点より、本件不正アクセスでは、攻撃者が管理者権限を行使し、多数の個人情報が保存されたファイル共有サーバーから各種ファイルを教育資料公開サーバーに収集、保存したことに照らせば、本件不正アクセスを受けての対応としてMENETに接続されていた校務系PCのクリーンインストールを行ったことは、合理的かつ必要なことであり、通常損害である。

争点②　原告の損害

【裁判所が認めた項目一覧③】

損害項目	理由
８．MENET学習系末端復旧作業業務委託料(4349万8080円)	7.で認定及び判断したのと同様（基準２の③の観点）、本件システムの個人情報保護ネットワーク内に設置されたドメインコントローラサーバに管理用アカウントで接続して、管理者権限を行使されたのであるから、それに接続されたタブレットＰＣについてもクリーンインストールを行うことは必要な対応であり、通常損害である。
９．連絡手段確保のためのノートPCリース代(248万6484円)	ＭＥＮＥＴは、インターネットへの接続を含めた市内各学校（園）、教育機関等を結ぶ情報通信ネットワークであること、基準２の②の観点による指摘を踏まえ、本件不正アクセスを受けての対応として、原告がＭＥＮＥＴのネットワークをインターネットから切断しサービスを停止することは、必要なものであり、かつ、これにより情報通信ネットワークが一時的に遮断されるため、各学校への最低限の連絡手段の確保をして事業継続を行うに当たって、上記のノートＰＣのリースやリースアウトＰＣのクリーンインストールを行うことは必要かつ相当なものといえ、通常損害である。

争点②　原告の損害

【裁判所が認めた項目一覧④】

損害項目	理由
10．MENET再構築業務委託料(1653万4866円)	原告は、2019年1月16日頃、被告に対し、ＭＥＮＥＴ再構築業務の報酬として3913万9200円を支払ったが、その内の2260万4314円は、ＭＥＮＥＴの機能の追加又は増強に係る費用であったことが認められる。 ＭＥＮＥＴを本件不正アクセス以前の状態に再構築すること自体は、その内容に照らし、被告の債務不履行と相当因果関係のある通常損害であることは明らかというべきであるが、他方で、ＭＥＮＥＴの機能の追加又は増強に関係する部分については、被告の債務不履行と相当因果関係のある損害であると認めることはできない。(**一部認容**)
11．弁護士費用(1299万8222円)	原告が求めている損害は、いわゆる**拡大損害**であり、その主張立証に当たっても、同様にシステム開発に係るある程度の専門的知見を要するものと認められるのであり、このような事案の内容に照らせば、本件は、弁護士に訴訟追行を委任しなければ十分な訴訟活動をなしえない。 原告が本訴事件の訴訟追行を弁護士に委任したことにより要した**弁護士費用は、事案の難易、請求額、認容された額その他諸般の事情を斟酌して相当と認められる額の範囲内のものに限り**、被告の債務不履行と相当因果関係がある損害というべきであり、損害と認定された合計額（1億2998万2222円）の**約1割**を認めるのが相当である。

争点②　原告の損害

【裁判所が認めなかった項目一覧】

損害項目	理由
１．MENET再構築に関する情報セキュリティ支援業務委託料(218万8400円)	本件不正アクセスの再発防止を主眼とするものであり、ＭＥＮＥＴの機能の追加又は増強に係るものと認めるのが相当であり、これは、ＭＥＮＥＴを本件不正アクセス前の状態に戻すために必要なものとはいえないから、通常損害ではない。
２．C学校校内ネットワーク再構築業務委託料	独自ネットワークを構築していたC学校の機器は、そのネットワークに独自のセキュリティ機能があることが推認できることに照らせば、MENETと接続している状態であったことから、直ちに、校内PCのクリーンインストールを行い校内ネットワークの再構築をする必要があったとまでは認め難く、通常損害ではない。
３．学校評価システム共有フォルダ利用型構築作業業務委託料	独立したサーバである学校評価システム共有フォルダ利用型の再構築が必要と認められず、通常損害ではない。
４．指導者用タブレットPC周辺機器購入費用	タブレットPC周辺機器がなければ従来の作業効率を確保できないとの事実は認めらず、通常損害ではない。
５．DNSサーバー移行費用	本件不正アクセスを契機としてDMZネットワークを撤去する必要があるとする証拠は見当たらず、通常損害ではない。

争点③　責任限定契約の適用の有無（抗弁）

【被告の主張】

原告との間で、平成２７年５月１１日、本件委託契約の１７条の規定により、同契約における被告の損害賠償責任の範囲につき、契約金額を限度として現実に生じた通常の直接損害を賠償するものとする旨の契約（本件責任限定契約）をしており、**被告が賠償すべき損害は、本件委託契約の契約金額である１億０４８０万０５００円が限度**となる。

【裁判所】

被告が、権利・法益侵害の結果について故意又は重過失がある場合にまで、当該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いうことは著しく衡平を害するものであり、当事者の通常の意思に合致していないというべきであるから、**本件委託契約の１７条は、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。

（東京地裁平成２６年１月２３日判決・判例時報２２２１号７１頁参照）。

被告は、原告との間で、本件委託契約の前後における提案依頼書、提案書、要件定義書、設計方針及び基本設計書において、外部ファイアウォールないし内部ファイアウォールによる外部からのアクセス制限を行うことを複数回にわたって確認していたことが認められるから、被告が原告に対して不適切な設定のまま本件システムを引き渡したことは、**単純かつ明白なミスであるというべき**であり、かつ、被告が情報セキュリティについて高度な専門的知見を有していることを併せ考えると、被告には本件委託契約の債務不履行について**少なくとも重過失があることは明らか**というべき、として責任限定契約の適用を否定した。

３．関連裁判例

1【商品の受注システムの不具合により顧客のクレジットカード情報が流出した事案において、会社のシステム会社に対する損害賠償請求が認められた事案】（東京地判平26・1・23）

・SQLインジェクション攻撃の事例
当事者間で明示のセキュリティ対策の合意が無い場合に、システム会社が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かが争われた事例

・裁判所の認定
① 「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。」

②「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」

・損害
①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（QUOカード送付等）
③顧客からの問い合わせ等の対応費用　493万8403円
④調査費用　393万7500円
⑤データセンタ使用料　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

2【会社のインターネット上で提供する車、バイクの一括査定システムにおいてSQLインジェクションの攻撃を受けた事案において、会社のシステム会社に対する損害賠償が認められた事案】（東京地判平30・10・26）

・SQLインジェクション攻撃の事例
当事者間の確認書においてシステム制作においてセキュリティの十分の確保、個人情報流出対策の十分の確保、既知の脆弱性としてSQLインジェクションが明記されていた事例

・裁判所の認定
平成24年当時、すでにSQLインジェクションによる不正アクセス等のセキュリティ上のリスクの存在が広く知られ、その対策としてエスケープ処理の実施という具体的な方法もシステム開発の業界では周知されており、SQLインジェクションに対する対策を講ずべき注意義務があったのにこれを怠っていたのであり、少なくとも過失による不法行為が成立。

・損害
①調査及び対策費用　47万5200円
②サーバ移転費用　35万6400円
③2日間の休業損害　11万9495円

３【当事者間の業務委託の内容にセキュリティ対策業務が含まれていたとはいえないとされ、会社のホームページ制作等会社に対する損害賠償請求が認められなかった事案】（東京地判令1・12・20）

・当事者間の契約内容が争われた事案

・裁判所の認定
本件契約における当事者の合意内容をうかがわせる本件注文書に委託される業務として記載された「本件サイトの運用，保守管理」との記載は，本件サイトが直ちに本件システム全体を意味するとまではいえない以上は，少なくともその文言上，これに本件システム全体を対象とする業務が含まれることが直ちに読み取れるとまでいうことはできず，また，同じく本件注文書に委託される業務として記載された「Ｄ１カスタマイズ」との記載についても，Ｄ１はインターネット上の通販サイト用のソフトウェアの一つである一方，Ｅ１はインターネット上の暗号化通信に用いられるオープンソースソフトウェアであり，両者は全く性質の異なるソフトウェアであることから，このような記載に係る業務にＥ１に関するセキュリティ対策業務が含まれている旨を直ちに読み取ることも困難であって，Ｄ１においてＥ１を経由した通信がされるからといって，Ｄ１のカスタマイズ業務の委託を受けた者が，当然にＥ１に関するセキュリティ対策業務の委託を受けたこととなると解することはできない。

４【会社の運営するECサイトからの顧客クレジットカード情報漏洩につき、損害賠償請求が認められなかった事案】（東京地判令2・10・13）

・本件決済モジュールにつき問題が生じ、当事者間の契約内容が争われた事案

・裁判所の認定
　①本件決済モジュールは，Ｅ社が開発し，Ｄ社が提供していたものであるから，被告は，本件決済モジュールの設計を行う開発者には該当しないというべきである。
　②本件請負契約に基づく被告の具体的な業務内容は，本件請負注文書の内容によって定まっていたものと認められる。本件請負注文書において，被告は，本件サイトにおけるクレジットカード決済機能を「導入」するものとされ，同機能を開発し，又は同機能を提供するプログラムを製作するものとはされていなかった。そして，前記認定事実のとおり，原告は，被告に対し，本件サイトのショッピングカート機能について，旧カートシステムを□□独自のシステムへと変更したいとの意向を伝えた上，４万円（消費税別）の代金に相当する作業を請け負わせたもので，本件請負注文書の他の項目をみても，被告が本件サイトにクレジットカード決済機能を提供する何らかのプログラムを開発する旨の記載は存在しない。そうすると，被告は，本件決済モジュールの開発を行う開発者には該当しないというべきである。

③被告は，本件決済モジュールについて，□□を利用した本件サイトにインストールし，原告から提供を受けたアカウント情報を用いて設定を行い，テスト環境において正常な決済ができることを確認したにとどまり，本件決済モジュールの機能を追加し又は変更するプログラムを製作したものではない。そして，本件決済モジュールのソースコードの修正についても，被告は，本件サイトの構築又は稼働に必要な限度で，モジュールのソースコードのうち，「テンプレート」と呼ばれる，ウェブページの構造やデザインに関する力を行う部分を修正したにとどまり，D社のサーバーとの通信を含めクレジットカード情報の処理を行う部分の修正は行っていない。そうすると，被告は，本件決済モジュールのカスタマイズを行う開発者には該当しないものというべきである。本件決済モジュールの設計，開発及びカスタマイズを行う開発者に該当しないにもかかわらず，相当額の対価の支払を受ける約定もないのに，高度の専門的知見と相当のコストを要する作業を進んで請け負うことは考え難い。本件サイトに顧客のクレジットカード情報を保存しないことが，原告及び被告の共通認識となっていたとみられることを考慮しても，本件請負契約に関し，原告と被告との間で，被告が，本件決済モジュールのソースコードや，同モジュールが生成するログを調査し，同モジュールが，セキュリティ脆弱性を有しないか，異常処理を生じさせないかといった点を確認する義務を負うとの合意をしていたことを認めることはできない

４．情報セキュリティ・サイバーセキュリティ関連参考資料

情報セキュリティ・サイバーセキュリティに関する主要な資料

- **情報セキュリティとサイバーセキュリティ**
  - **情報セキュリティ**：情報を守るためのセキュリティ。情報が保存される媒体を問わない。
  - **サイバーセキュリティ**：電子化された情報を守るためのセキュリティ。

- **情報処理推進機構(IPA)発行**

1．情報セキュリティ10大脅威2024：2023年に発生し社会への影響が大きかったと考えられる情報セキュリティ関連事案から10大脅威を選定（2014年から毎年実施）。2023年の1位は「ランサムウェアによる被害」が選出された。
2．情報セキュリティ白書2024：情報セキュリティに関する国内外の政策や脅威の動向、インシデント発生状況、被害実態などをまとめた資料（毎年発行）
3．サイバーセキュリティ経営ガイドライン Ver 3.0：経営者の主導のもとで組織的なサイバーセキュリティ対策を実践するための指針をまとめた資料
4．サイバーセキュリティ経営ガイドラインVer3.0実践のためのプラクティス集 第4版：３.の資料をより実践的に理解するために作成された資料。具体的な取り組み事例などが紹介されている
5．情報システム・モデル取引・契約書（第二版）：**セキュリティ条項(第50条)**が大幅に加筆された

- **内閣サイバーセキュリティセンター（NISC)発行**

ーサイバーセキュリティ関係法令Q&AハンドブックVer.2.0：サイバーセキュリティに関連する法令をQ&A形式で解説する資料

５．ディスカッションポイント

ディスカッションポイント

1　システム開発におけるセキュリティについて、ベンダーが負う責任について

裁判所は、委託契約に基づき外部ファイアウォールと内部ファイアウォールを適切に設定することにより通信制限を行うべき債務を負っていたかについて負う旨の認定をしている。

裁判所の考え方は、
①契約書記載の内容のみならず、
②記載がない場合であっても、同契約の前後にやり取りがなされた要件定義書や基本設計書などの内容を総合的に考慮して確定すべきである

そのうえで、以下の３点を理由にあげ、債務を負っていた旨認定している。
①提案依頼書、提案書、要件定義書及び基本設計書には、外部ファイアウォール及び内部ファイアウォールにより通信制限を行う旨の記載
②設計方針及び基本設計書には、データセンター内理論接続図及び通信制限イメージにおいて、ＤＭＺネットワークと個人情報保護ネットワークとをつなぐ通信経路が存在しないこと
③被告は、経験豊富な専門家を多数擁する技術的セキュリティ対策チームによる総合的なセキュリティソリューションを提供することを可能とする技術力を有していた

Ｑ１　このような裁判所の考え方に賛成か

Ｑ２　今回の事案は、①や②を理由に債務を負っていた旨を認定しているが、例えば、要件定義書等にも記載がないセキュリティの問題についても、ベンダーはセキュリティを適切に設定する債務を負うのか
（関連裁判例①）において、裁判所は「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。」旨判示している。
そうだとすると、専門家としてある程度の責任を負い、セキュリティを適切に設定する債務を負うか

Ｑ３　その当時の技術水準として経産省やＩＰＡの基準が使われているが、どのような基準があると判断しやすいか

Ｑ４　③を理由に債務を負っていた旨を認定しているが、例えば、ＮＴＴ東日本のような総合的なセキュリティソリューションを提供することを可能とする技術力を有していないベンダーの場合でも、今回の案件と同じようにベンダーとしての債務を負うのか、それともベンダーの規模によって債務は異なってくるのか

２　争点①―２に関連して「被告の債務不履行に係る帰責事由の不存在」について

　ベンダーの「納品した完成図書には、外部ファイアーウォール及び内部ファイアーウォールについて実際にされた設定が記載されており、原告はその設定について了解ないし認識していた」「検収していた」旨の主張に対し、裁判所は「交付を受けた者がその全体をみて本件システムが自らの要求を満たすものであるか否かを確認することは現実的に困難であり、不可能に等しいもの」「不適切な設定になっていることは想定し難い事実」と認定し、ベンダー側に責めに帰すべき事由がないということはできない旨判示している。

Ｑ１　裁判所の認定に賛成か

Ｑ２　裁判所は「原告に対してファイアウォールの不適切な設定について告知ないし説明をしていたというのであれば格別」「原告と被告との間のコンピュータシステムの構築などの専門性には相当の格差がある」としているが、ベンダーはユーザに対し、どの程度の説明をする必要があるのか

Ｑ３　ユーザが会社、教育委員会、個人等によって説明の義務の程度は変わってくるのか

Ｑ４　ユーザ側の責任も考慮すべきか、今回の場合であれば、ベンダーが通信設定について事前に問い合わせをしていたにもかかわらず、ユーザ側が把握していなかった事情、または、ユーザが協力的でない状況の場合（セキュリティについて費用をかけたくない等）

３　損害の範囲の認定について

裁判所は、①デジタルフォレンジック対応業務委託料②インシデント対応支援コンサルティング業務委託料③保護者教職員宛て郵送料④職員時間外勤務手当⑤第三者委員会報酬⑥外部ネットワーク調査委託料⑦校務末端復旧作業委託料⑧学習系末端復旧作業委託料⑨ノートPCリース代⑩再構築業務委託料⑪弁護士費用について認めている。
その基準として、①インシデント情報の検知②インシデント情報の分析（トリアージ）③初動対応及び証拠保全④当局対応及び情報開示⑤原因分析及び再発防止⑥事後対応（被害者への補償、被害回復及び責任追及）を採用している。

Ｑ１　裁判所の判断に賛成か

Ｑ２　より認められるべきという考え方はあるか

Q3　セキュリティ事故に基づく損害は広範になることが考えられ、損害をより制限的に考えるべきとも考えられるか

4　セキュリティ事故を防止するためにどのような策があるか

・契約書にセキュリティ仕様を明確に記載することが効果的か、そのほかの策があるか。

発表を終えて

１．ディスカッションのハイライト

- 裁判所の判断については、参加者全員が賛成の見解だった。被告の「本件システムの提供に当たり、その外部ファイアウォール及び内部ファイアウォールを適切に設定して通信制限を行う債務」を認めた判断につき、委託契約の性質や当該契約の前後に取り交わした書類内容を踏まえた認定は納得できるとの意見が多かった。被告がなぜファイアウォールの設定を不適切な状態で納品してしまったのか、また、「検証報告書」を参照した上で、原告側が本件システムの納品日と同日に検収を完了することは妥当といえるのか、原告側の受け入れ態勢に不備があるとして過失相殺の主張はされなかったのはなぜか、といった本事件が発生した経緯や主張につき腑に落ちない点があるとの意見も見られた。

- 裁判所が「原告に対してファイアウォールの不適切な設定について告知ないし説明をしていたというのであれば格別」と示した点につき、どの程度被告が説明をすれば足りたのかどうかは、リスクがある状態であることを認識していた被告としては、少なくともそのリスクを原告が認識できる程度には説明すべきだったとの意見が多かった。

- 損害に関し、本件不正アクセスにより個人情報が流出した可能性のある個人への補償（損害）まで請求しなかった理由は、裁判実務上、補償額が少額であるためなのかといった意見、また、本件不正アクセスの対応に職員が時間外勤務を行なうことで生じた手当まで認定しているが、人件費は業務遂行上発生する性質のため認定しづらい傾向がある中で、本件では通常は負担する必要のない費用であり、被告が負担べき費用との見解は実務上、参考になるといった意見もあった。

- 本事件のようなトラブルを未然防止する措置について、セキュリティレベルの仕様は、ユーザ予算の中で定める他なく、ユーザ側がセキュリティ技術に精通しているかどうかにかかわらず、ベンダーは、専門家として、受発注時、引渡し時などにおいて、ユーザに対し、提供するセキュリティ仕様の効果やリスクを明確に説明し、ユーザ側と認識合わせをすることが肝要ではないか、との意見が挙がった。特に、非機能要件であるセキュリティ仕様は、機能要件に比べて、後回しにされがちではあるが、昨今のサイバーセキュリティリスクの高まりや個人情報保護意識の高まりを前提に、ベンダーだけでなくユーザ側も理解をしていく必要があるといった意見もあった。

２．報告者の所感

●伊藤

- セキュリティの不備が結果的に委託契約の契約金額を超える損害賠償責任を認めた裁判例として、ベンダー業界は他山の石とせず、反面教師として認識すべき事件であると感じた。
- セキュリティ設定（非機能要件）の不備は、システムが動かないという事態等に陥らない限り、ユーザは容易に認識できるものではなく、また、当該セキュリティ設定を放置する合理性が見出せない以上は、ユーザが検収を行ったとしても、ベンダーが責任を負う他ないとの見解につき、納得した。

●土方

- この案件においてベンダーの債務が何であったのか、債務不履行構成を採るなかで改めて考える必要があると感じた。
- ベンダー側とユーザ側の意見の双方を聞きながら、コミュニケーションの重要性を感じるとともに、ベンダー側からのアプローチの重要性を認識した。