〔論　説〕

日本における民事サイバーセキュリティに関する判例法を探る

松　尾　剛　行

Ⅰ　はじめに

１　サイバーセキュリティの重要性

サイバーセキュリティ[1]の重要性がますます認識されるようになっている。とりわけ，個人情報漏洩事故，不正アクセス，ランサムアタック等の企業を取り巻くセキュリティに関する問題が注目を集めている[2]。

２　本稿の趣旨

このような状況下において，民事サイバーセキュリティに関する裁判例を集約・分析することを通じて，サイバーセキュリティに関する実務上有用と思われる教訓の抽出を試みたい。

とりわけ，①いわゆるベネッセ事件から約 7 年が経過し，主な裁判例も出揃っていることから，同事件の裁判例からみる，個人情報の保護や委託に関する責任に関する教訓を抽出し（Ⅱ），また，②複数の企業間において情報セキュリティに関する責任の分担に関する基準が問題となった裁判例からそのような問題に関する裁判例の考え方を抽出し（Ⅲ），最後に，③サイバーセキュリティにおけるいわゆる CIA 毎に，それぞれが問題となった事例を紹介したい（Ⅳ）。

３　本稿で検討しないもの

ここで，サイバーセキュリティに関する裁判例は実際には多数存在するところ，紙幅の関係で，本稿では，刑事[3]，行政[4]，労働[5]，オフラインのセキュリテ

---

1)　セキュリティの法律問題については，岡村久道『情報セキュリティの法律』（商事法務，改訂版，2011 年），塩崎彰久ほか編著『サイバーセキュリティ法務』（商事法務，初版，2021 年）及び「サイバーセキュリティ関係法令 Q&A ハンドブック」内閣サイバーセキュリティーセンター<https://www.nisc.go.jp/security-site/files/law_handbook.pdf>（2021 年 8 月 29 日最終アクセス，以下同じ。）2020 年 3 月 2 日公表等参照。

2)　情報処理推進機構（以下「IPA」という。）は「情報セキュリティ 10 大脅威 2021」として，組織については「ランサムウェアによる被害」「標的型攻撃による機密情報の窃取」「テレワーク等のニューノーマルな働き方を狙った攻撃」を上位 3 番目までに挙げている。「情報セキュリティ 10 大脅威 2021」IPA <https://www.ipa.go.jp/security/vuln/10threats2021.html>。

3)　典型例が，ベネッセ刑事事件（東京高判平成 29 年 3 月 21 日判タ 1443 号 80 頁）である。なお，刑事手続法につき，越境捜索を適法とした最決令和 3 年 2 月 1 日裁判所時報 1761 号 4 頁も参照。

4)　典型例が，住基ネット訴訟（最判平成 20 年 3 月 6 日民集 62 巻 3 号 665 頁）である。

5)　例えば，業務上インフラ・ネットワークシステムの管理等の業務を担当していた従業員について，会社からのアクセス権限の修正について（抽象的な）指示がされていたものの，その指示に従わなかったと主張された事案において「当該業務の内容は多岐にわたる上，インフラ・ネットワークシステムの性質上，これに何らかの変更を加える場合には，その変更が他の従業員に大きな影響を与えることがあり得るのであって，原告（注：従業員）の一存のみでその時

ィ[6]等[7]の類型の裁判例は検討しないこととする。

Ⅱ　ベネッセ事件に見る個人情報漏洩事故とセキュリティ

1　はじめに

ベネッセ事件に関する民事裁判例のうちデータベース等で発見できたものは以下の表1のとおり，9系列18裁判例である。そして，表1から分かるように，いわゆる判例雑誌等に搭載された公刊裁判例のみでは，到底これらの裁判例を網羅的に理解することができず，本稿において行うようなデータベース（のみ）搭載裁判例を含む検討が重要と言える。ただし，細かなものを含めば論点が多いことから，以下では，主に個人情報を取り扱う業者（ベネッセ）とその委託先（シンフォーム）が「どのようなセキュリティ対策を講じる義務を負う」と解されているのかという観点にフォーカスしたい。

・東京高判令和3年5月27日第一法規28291776（原審：東京地判平成31年4月25日第一法規28271746）
・東京高判令和3年3月17日第一法規28290858（原審：東京地判令和元年9月6日第一法規28273526）
・東京高判令和2年3月25日第一法規28281108（原審：東京地判平成30年12月27日判例タイムズ1460号209頁）
・東京高判令和2年3月25日裁判所HP（原審：東京地判平成30年6月20日第一

期や内容を決定できるものではないことは容易に推認することができるから，仮に共有フォルダのアクセス制限の修正について被告（注：会社）から抽象的な指示があったとしても，そのことをもって原告に具体的な債務が発生したということはできない」とした東京地判平成26年11月14日第一法規29043691参照。なお，筆者は季刊労働法274号（2021年）に「テレワークにおけるプライバシーの法的課題」を寄稿しており，労働関係のプライバシーにつき，『プライバシー法（仮称）』（弘文堂，共著）においても研究成果を公表予定である。

[6] 例えば，家庭裁判所調査官による少年のプライバシーに関する事項の公表が問題となった最判令和2年10月9日民集74巻7号1807頁参照。

[7] なお，金融関係については，最近暗号資産等に関し興味深い裁判例が多数公表されているところであり，この問題については他日を期したい（なお，一般的な決済サービスと関係する広義のセキュリティが問題となった裁判例については吉本利行『判例に学ぶ決済サービスの法務と実務』（金融財政事情研究会，初版，2021年）が参考になる。）。また，ベネッセ事件株主代表訴訟（広島高岡山支判令和元年10月18日第一法規28280260（原審：岡山地判平成30年9月12日裁判所HP））においては，内部統制・ガバナンスとセキュリティの問題が提起されているが，この問題も他日を期したい。

法規 28262746） ・東京高判令和元年 6 月 27 日判例時報 2440 号 39 頁（原審：東京地判平成 30 年 6 月 20 日判例時報 2440 号 45 頁） ・東京高判令和元年 6 月 27 日裁判所 HP（原審：横浜地判平成 29 年 2 月 16 日第一法規 28273142） ・京都地判令和 3 年 1 月 19 日裁判所 HP ・千葉地判平成 30 年 6 月 20 日判例時報 2399 号 46 頁，判例タイムズ 1459 号 186 頁 ・最判平成 29 年 10 月 23 日判例時報 2351 号 7 頁，判例タイムズ 1442 号 46 頁（差戻審：大阪高判令和元年 11 月 20 日判例時報 2448 号 28 頁，原審：大阪高判平成 28 年 6 月 29 日判例時報 2351 号 9 頁，判例タイムズ 1442 号 48 頁，原々審：神戸地姫路支判平成 27 年 12 月 2 日判例時報 2351 号 11 頁，判例タイムズ 1442 号 50 頁）

表 1：裁判例一覧

まず，主要な争点に関する裁判例の結論をまとめると表 2 の通りとなる。

	ベネッセの注意義務違反	シンフォームの注意義務違反	シンフォームの使用者責任	損害（慰謝料[8]）
神戸地姫路支判平成 27 年 12 月 2 日（最判平成 29 年 10 月 23 日の原々審）	×	当事者とされていない		注意義務違反なし
大阪高判平成 28 年 6 月 29 日（最判平成 29 年 10 月 23 日の原審）	損害を先に否定			×
横浜地判平成 29 年 2 月 16 日（東京高判令和元年 6 月 27 日の原審）	×			注意義務違反

8) 弁護士を代理人に立てた原告については，慰謝料に加え，概ね損害総額の 10%が弁護士費用として認められる。なお，1000 円の弁護士費用を認めたものとして，上記東京高判令和 3 年 5 月 27 日がある。また，慰謝料以外の損害を認めたものとして，上記京都地判令和 3 年 1 月 19 日は，漏えいした項目を確認するための内容証明郵便送料，異議申し立て文書送付代等合計 1960 円を損害として認めている。

				なし
最判平成 29 年 10 月 23 日	（判断せず）			差戻し
東京地判平成 30 年 6 月 20 日 （東京高判令和 2 年 3 月 25 日の原審）	○	○	×	×
東京地判平成 30 年 6 月 20 日 （東京高判令和元年 6 月 27 日の原審）	○	○	×	×
千葉地判平成 30 年 6 月 20 日	×	当事者とされていない		注意義務違反なし
東京地判平成 30 年 12 月 27 日 （東京高判令和 2 年 3 月 25 日の原審）	×	×	○	3000 円
東京地判平成 31 年 4 月 25 日 （東京高判令和 3 年 5 月 27 日の原審）	×	×	○	3000 円
東京高判令和元年 6 月 27 日 （原審：東京地判平成 30 年 6 月 20 日）	○	○	×	2000 円
東京高判令和元年 6 月 27 日 （原審：横浜地判平成 29 年 2 月 16 日）	○	○	×	2000 円
東京地判令和元年 9 月 6 日 （東京高判令和 3 年 3 月 17 日の原審）	○	○	×	3000 円
大阪高判令和元年 11 月 20 日 （最判平成 29 年 10 月 23 日の差戻審）	○	当事者とされていない		1000 円
東京高判令和 2 年 3 月 25 日 （原審：東京地判平成 30 年 12 月 27 日）	○	○	×	3000 円
東京高判令和 2 年 3 月 25 日 （原審：東京地判平成 30 年 6 月 20 日）	○	○	×	3000 円
京都地判令和 3 年 1 月 19 日	○	○	判断不要とされる	1000 円
東京高判令和 3 年 3 月 17 日	○	○	×	3000 円

（原審：東京地判令和元年 9 月 6 日）				
東京高判令和 3 年 5 月 27 日 （原審：東京地判平成 31 年 4 月 25 日）	○	○	仮に認められても右記を上まわる損害はないとされる	3000 円

表 2：裁判例まとめ

２　前提となる事実関係の概要

ベネッセ事件についてはその概要をご存知の読者は多いと思われるが，裁判例を理解する上で最低限必要な内容について以下のとおり要約した（以下の記載は主に裁判例の認定事実による）。

ベネッセは，関係会社であるシンフォームに IT 業務を委託していた[9]。シンフォームは IT 業務を実施する上でその一部の業務を A に委託していた。A は，シンフォームと雇用契約を締結していない。ただ，シンフォームのグループリーダーの配下に属して当該委託業務に従事していた。平成 25 年 7 月頃から平成 26 年 6 月頃にかけ，A は，USB ケーブルを用いて業務用パソコンの USB ポートに MTP 方式の通信に対応したスマートフォンを接続し，MTP 通信でデータを転送する方法によって，ベネッセが保管していた個人情報を不正に取得し，これを名簿業者等へ漏洩させた。漏洩した個人情報は，子及び親の氏名，性別，生年月日，郵便番号，住所及び電話番号等である。そして，当時ベネッセに対する個人情報保護法に関する監督官庁であった経済産業省は，2014 年（平成 26 年）9 月 26 日に，ベネッセに対して個人情報の保護に関する法律（以下「個人情報保護法」という。）違反（安全管理措置義務違反及び委託先の監督義務違反）を認めて勧告をしていた。

なお，やや技術的であるものの，裁判所の認定で問題となった点として，スマートフォンと PC 間の通信方式がある。スマートフォンと PC 間の通信方式につ

9)　元々ベネッセはシンフォームの親会社であり，その後持ち株会社化し，双方がベネッセホールディングスの 100%子会社（つまり両社の関係は兄弟会社）となっている。

いては，主なものとしてMSC方式とMTP方式があり，過去の時点においてはMSC方式が用いられることが多かったが，その後MTP方式も徐々に増加した。本件当時，シンフォームが採用したセキュリティソフトは，MSC方式での書き出しに対しては，これを制御する機能が存在した。そして確かに，当該セキュリティソフトを利用した上で，適切に設定をすればMTP方式の書き出しを禁止することもできたものの，当該セキュリティソフトでは，スマートフォンのMTP方式の通信のみを選択的に制御することができず，デジカメ等も含め包括的に書き出しを禁止する結果になってしまう。そして，シンフォームは実際には，当該セキュリティソフトを利用してMTP方式での通信を禁止する設定をしていなかった。そのような状況下で，AはMTP方式のスマートフォンを業務用PCに接続することで個人情報を取得したものである。

３　ベネッセ・シンフォームが負うべき責任とその根拠

民法715条1項[10]は使用者に対し，「被用者がその事業の執行について第三者に加えた損害を賠償」する責任（使用者責任）を負わせる。そこで，Aとシンフォームの間に「被用者」と使用者の関係が存在すればシンフォームはAの行為につき使用者責任を負い得る。

また，民法709条[11]は各主体に過失があれば，それによる権利又は法律上保護される利益の侵害に対して責任を負うとする。よって，シンフォームの過失及ベネッセの過失もまた別途問題となり，これらが認められる主体については，不法行為責任を負う可能性がある。

ここで，個人情報保護法22条[12]は個人データの取扱いを委託する場合に，委託者側に受託者の監督義務を負わせている。ただし，これは公法上の規制であり，ただちに民法709条等における注意義務その他の私法上の義務と同一とは言えないと解されている[13]。

---

10)「ある事業のために他人を使用する者は，被用者がその事業の執行について第三者に加えた損害を賠償する責任を負う。ただし，使用者が被用者の選任及びその事業の監督について相当の注意をしたとき，又は相当の注意をしても損害が生ずべきであったときは，この限りでない。」

11)「故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は，これによって生じた損害を賠償する責任を負う。」

12)「個人情報取扱事業者は，個人データの取扱いの全部又は一部を委託する場合は，その取扱いを委託された個人データの安全管理が図られるよう，委託を受けた者に対する必要かつ適切な監督を行わなければならない。」

13) 松尾剛行「最新判例にみるインターネット上のプライバシー・個人情報保護の理論と実務」（勁草書房，初版，2017年）244頁以下参照。

なお，単に個人情報が漏洩したとしても，それだけで「権利又は法律上保護される利益を侵害した」といえるかや，損害が発生しているといえるか等という問題が存在した。最高裁は，上記最判平成 29 年 10 月 23 日において，氏名，性別，生年月日，郵便番号，住所及び電話番号等であっても「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」ところ，名簿業者等への漏洩といった本件の事実関係によれば，プライバシーが侵害されたと言える以上，精神的損害の有無及びその程度等について十分に審理すべきであったと判示している。

以下，自らの個人情報が漏洩する被害にあった被害者が原告となり，ベネッセ及びシンフォームを被告として訴えた（ただし，表 2 のとおり，一方のみが被告となっている場合がある）一連の訴訟の判決における，これらの点についての判断を，各系列の最終審に関する 9 つの判決から見ていくこととする。ただし，原審と控訴審で判断が分かれたものも多く，一部は原審の判断についても補足している。

４　東京高判令和 3 年 5 月 27 日（原審：東京地判平成 31 年 4 月 25 日）

（1）シンフォームの注意義務違反

シンフォームにおいて，本件当時において MTP による通信方法を含め，これに対応したスマートフォンを利用した情報漏えいがあり得ることの予見可能性は十分存したというべきとした上で，執務室内への私物スマートフォンの持込禁止は，簡便かつ確実に行うことができる情報漏えい防止の方法ということができ，これによって，悪意のある内部者による情報流失を防ぐことが可能であるとして，シンフォームに執務室内への私物スマートフォンの持込禁止措置を講じる義務があったとした。シンフォームは，業務への支障を主張したが，個人情報の流失の危険に比して，執務室内での私物スマートフォンを使用することによる便宜が上回るような具体的な事情があったとも認められないとしている。また，シンフォームにおいて，本件当時，MTP 対応スマートフォンによる個人情報の漏えいの危険性について認識し得たところ，セキュリティソフトの導入目的は，情報漏えい防止であり，さらに，私物スマートフォンの持込禁止措置と異なり，書き出し制御措置はシンフォームにおいて能動的に行うことができることからすると，本件当時，MTP スマートフォンを含めて書き出し制御措置を講ずべき注意義務があったとした。

（2）ベネッセの注意義務違反

ベネッセについては，個人情報保護法 22 条に基づく公法上の監督義務を背景に，被害者との関係においても，個人情報の提供先であるシンフォームを適切に監督して，個人情報が漏えいしないようにする注意義務があったとし，少なくともセキュリティソフトの設定が適切に行われているか否かの報告を求めて，その確認を行う義務があり，同義務を尽くしていれば，これによって漏えい行為を回避できたと認められるとして注意義務違反を認めた。

（3）損害その他について

ベネッセらにおいて一定の予防措置が講じられていること，漏洩発覚後の調査，報告，500 円相当の謝罪品の交付等の事情を踏まえ，3000 円の慰謝料が相当とした。

使用者責任が仮に認められるとしても，その認容額は（3）で述べる損害額を上回るものではないと判断された。

なお，原審は，シンフォーム及びベネッセの義務違反は否定したものの，A とシンフォームの間の指揮命令関係を認定し，使用者責任を認めた。

５　東京高判令和 3 年 3 月 17 日（原審：東京地判令和元年 9 月 6 日）

（1）シンフォームの注意義務違反

シンフォームが事業活動上取り扱う対象は顧客からの大量の個人情報であり，情報管理に関する社会一般の認識に照らしても情報セキュリティ対策に細心の関心を払うべき立場にあるとした上で，セキュリティソフトの設定を見直し，これを適切な設定に変更すべき注意義務があったところ，シンフォームはこれに違反したとした。

（2）ベネッセの注意義務違反

ベネッセについては，事業展開に伴って顧客の個人情報が大量に集積していることを前提に，かかる情報の取り扱いをシンフォームに委託するにあたり，顧客等に対しても，信義則上，委託先監督義務を負うとした。その上で，セキュリティソフトの設定が適切に行われているかどうかについて適切に報告を求めていれば，漏洩を回避できたとして注意義務違反を認定した。

（3）損害その他について

漏洩した情報は，秘匿する必要性が高い情報であるとはいえないところ，財産

的損害その他の実害が生じていることはうかがわれない点に加え，ベネッセらにおいて一定の予防措置が講じられていること，漏洩発覚後の調査，報告，500円相当のお詫びの品の交付等の事情を踏まえ，3000円の慰謝料が相当とした。

シンフォームの使用者責任は否定している。

なお，原審も控訴審と類似した枠組みを採っている。

６　京都地判令和3年1月19日

（1）シンフォームの注意義務違反

シンフォームとしてMTP対応スマートフォンによる漏洩の予見可能性はあり，執務室内に私物のスマートフォンの持込みを禁止する措置を講ずべき注意義務及び書き出し制御措置を含むMTP対応スマートフォン制御措置を講じるべき注意義務があったところ，これらを怠ったとした。

（2）ベネッセの注意義務違反

ベネッセについては，預かった大量の個人情報の管理について，その時々の情報セキュリティを取り巻く状況の変化に対応しつつ，委託先に対する適切な指導監督をすべき注意義務があったとした上で，セキュリティソフトのMTP対応スマートフォンの使用制御措置の設定変更，執務室内への個人スマートフォンの持込み禁止について適切に監督をすべき注意義務があったところ，これを怠ったとした。

（3）損害その他について

侵害態様，侵害された本件個人情報の内容及び性質，流出した範囲，実害の有無，個人情報を管理していた者による対応措置の内容等を踏まえ，慰謝料を1000円[14]と認定した。

なお，使用者責任については，損害が異なるとはいえないので判断不要とした。

---

[14]　なお，判決文においては，親権者の情報が子に関する情報として提供されているという事実も考慮されているとされているが，プラスに考慮されたのかマイナスに考慮されたかは明らかではない（同時期の他の裁判例と比較するとマイナスに考慮された可能性はある）。上記大阪高判令和元年11月20日のように親の情報は別のところで公開済みだということであれば（公開済みの）親の情報であることをマイナスに考慮することは十分理解できるが，単に親の情報だというだけでマイナスに考慮すべきかは疑問がある。

７　東京高判令和 2 年 3 月 25 日（原審：東京地判平成 30 年 12 月 27 日）

（1）シンフォームの注意義務違反

本件当時，シンフォームは，MTP による通信方法を含め，これに対応したスマートフォンを用いた個人情報のデータの転送があり得ることについても，想定することができたとして予見可能性を認めた。そして，直ちにスマートフォン持込禁止義務，USB 接続禁止義務等までは認められないものの，MTP 対応スマートフォンを含めて書き出し制御措置を講ずべき注意義務があったところ，シンフォームはこの義務を怠ったとした。

（2）ベネッセの注意義務違反

ベネッセについても，セキュリティソフトのスマートフォンに対する書き出しないし接続制御機能への対応状況について適切に報告を求める等の監督を怠ったとした。

（3）損害その他について

本件に現れた一切の事情を総合考慮し，慰謝料 3000 円を認めた。

シンフォームの使用者責任は否定した。

原審は，MTP 対応のスマートフォンによる不正取得は予見できないとしてベネッセ・シンフォームの過失を否定したが，A とシンフォームの業務実態に鑑み，シンフォームは，A の使用者であり，シンフォームは使用者責任を負うとした。

８　東京高判令和 2 年 3 月 25 日（原審：東京地判平成 30 年 6 月 20 日）

控訴審判決は上記 7 の東京高判令和 2 年 3 月 25 日の判断とほぼ同様である[15]。

原審は，シンフォームには，MTP 対応スマートフォンに対する書き出し制御措置を講ずべき注意義務があり，これを怠った過失があり，また，ベネッセにもセキュリティソフトウェアの変更について適切に監督をすべき注意義務を怠った過失がある（A に対する使用者責任は負わない）ものの，民法上，慰謝料が発生する程の精神的苦痛があると認めることはできないとした[16]。

---

15) 同じ東京高裁民事第 23 部による同日の判断である。
16) 下記 9 の東京高判令和元年 6 月 27 日の原審と同じ部の同一日の判決である。

９　東京高判令和元年 6 月 27 日（原審：東京地判平成 30 年 6 月 20 日）

（1）シンフォームの注意義務違反

デバイスや OS は，バージョンアップにより高機能化していくものであるから，それに応じて，接続されるデバイスを制御してデータの漏えいを防いでいく必要があるところ，ベネッセ・シンフォームは，セキュリティソフトを導入していたことに照らすと，このような必要性を具体的に認識していたと認めるのが相当としてMTP対応の本件スマートフォンを使用した漏えいについて予見可能性があったというべきとした。そして，シンフォームは，漏えいの発生以前において，MTP 対応スマートフォンに対する書き出し制御措置を講ずることが可能であったから，そのような措置を講ずべき注意義務があったにもかかわらず，これを怠った点に過失があったとした。

（2）ベネッセの注意義務違反

ベネッセにおいても，シンフォームに対し，MTP 対応スマートフォンに対する書き出し制御措置が講じられているか否かを確認すべく，セキュリティソフトの設定状況について適切に報告を求めていない点につき，監督義務を怠ったといえるとした。

（3）損害その他について

一切の事情を総合し，慰謝料 2000 円を認めた。

シンフォームの使用者責任は否定した。

原審は，シンフォームは，漏えい当時，漏えいと同様の方法で，個人情報が不正に取得されることを予見し得たところ，漏えい当時，MTP 対応スマートフォンを含むスマートフォンに対して書き出し制御措置を講じる注意義務があり，これに違反したとし，またベネッセは，シンフォームに対し，業務用パソコンのセキュリティソフトウェアのMTP対応スマートフォンに対する書き出し制御機能への対応状況について適切に報告を求めていなかったとした（使用者責任は否定）。しかし，「原告らに，民法上，慰謝料が発生する程の精神的苦痛があると認めることはできない」として損害賠償請求を棄却した[17]。

---

17)　上記 8 の東京高判令和 2 年 3 月 25 日の原審と同じ部の同一日の判決である。

１０　東京高判令和元年 6 月 27 日（原審：横浜地判平成 29 年 2 月 16 日）

（1）ベネッセの注意義務違反

ベネッセのみが被告とされていたところ，ベネッセは，シンフォームに対し，MTP 対応スマートフォンに対する書き出し制御措置が講じられているか否かを確認すべく，セキュリティソフトの設定状況について適切に報告を求めておらず，この点について監督義務を怠ったといえるとした[18]。

（2）損害その他について

一切の事情を総合し，慰謝料 2000 円を認めた。

原判決は，委託元の個人情報取扱事業者であるベネッセは，取扱いを委託する個人データの内容を踏まえ，本人の個人データが漏洩，滅失又は毀損等をした場合に本人が被る権利利益の侵害の大きさを考慮し，事業の性質及び個人データの取扱状況等に起因するリスクに応じた，必要かつ適切な措置を講じる義務があるところ，原告はベネッセが上記義務に違反したことを認めるに足りる具体的事実の主張・立証をする必要がある。しかし，このような具体的主張はされていない。反面，シンフォームは情報セキュリティマネジメントシステムの認定を取得しており，両社間の業務委託契約には，当該個人データの取扱いに関する，必要かつ適切な安全管理措置や委託された個人データの取扱状況を合理的に把握することを可能とする規定が盛り込まれており，かつ，ベネッセはシンフォームに対して定期的な監査は行っていたところ，その取り扱う情報が，漏洩した場合に二次被害が発生する可能性が高い個人データとまではいえないことに鑑みれば，このような委託先の選任・監督にかかる事実関係がシンフォームにおける委託された個人データの取扱状況を把握する義務に違反していたと認めるに足りる具体的な事実の主張も立証もないとしてベネッセの過失を否定した。

１１　千葉地判平成 30 年 6 月 20 日

ベネッセのみが被告とされていたところ，スマートフォンの転送形式やソフト開発は日進月歩であり，ある時点では書き出し制御システムが有効に機能しているとしても，その後の新たな技術等の開発によって，容易に当該システムが機能しなくなる可能性は当然に予見できるものであり，その他，ベネッセは，シ

---

18)　上記 9 の東京高判令和元年 6 月 27 日（原審：東京地判平成 30 年 6 月 20 日）と同じ部の同一日の判決である。

ンフォームにおいて，正規のアクセス権限を有していた者が，データベースから個人情報を大量に取得し，それを何らかの方法で外部へ持ち出し，漏えいする可能性があること自体については予見可能であったということができるとした上で，一般的な情報漏洩回避義務（通常の企業に要求された一般的水準における，情報漏えいの結果を回避すべき義務）[19]は認定できるとした。その上で，アラートシステム設定義務，書き出し制御義務，持ち込み禁止義務，アクセス権限細分化義務，ログ確認義務，責任と権限明確化義務等，原告の主張する具体的な義務違反について検討したものの，結論として全ての義務違反を否定した。

１２　最判平成 29 年 10 月 23 日（差戻審：大阪高判令和元年 11 月 20 日，原審：大阪高判平成 28 年 6 月 29 日，神戸地姫路支判平成 27 年 12 月 2 日）

（1）最高裁判決について

損害の発生を否定した下級審の判断[20]に対し，上記最判平成 29 年 10 月 23 日は，「本件個人情報は，上告人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ころ（最高裁平成一四年(受)第一六五六号同一五年九月一二日第二小法廷判決・民集五七巻八号九七三頁参照[21]），上記事実関係によれば，本件漏えいによって，上告人は，そのプライバシーを侵害されたといえる。しかるに，原審は，上記のプライバシーの侵害による上告人の精神的損害の有無及びその程度等について十分に審理することなく，不快感等を超える損害の発生についての主張，立証がされていないということのみから直ちに上告人の請求を棄却すべきものとしたものである。そうすると，原審の判断には，不法行為における損害に関する法令の解釈適用を誤った結果，上記の点について審理を尽くさなか

19)　具体的予見可能性については，MTP スマートフォンへのデータの書き出しを防止するには，従来のスマートフォンとは異なる対策を講じる必要があるということは，本件当時，一般的に認識されていなかったことが認められるから，ベネッセは，シンフォームにおいて，正規のアクセス権限を有していた者が，その所有するスマートフォンをクライアントパソコンに USB ケーブルで接続することによりクライアントパソコンからスマートフォンにデータを転送する方法によって，個人情報を不正に取得することを予見することはできなかったとした。このような具体的予見可能性が否定されたことが，結果的に義務違反が認定されなかった大きな理由であると理解される。

20)　原々審は「原告の氏名の情報が流出（漏えい）したのが，被告の過失行為によるものであることについて，これを基礎付けるに足りる具体的事情の主張立証がな」いとした。原審は「不快感や不安を抱いただけでは，これを被侵害利益として，直ちに損害賠償を求めることはできない」ところ「本件漏えいによって，控訴人が迷惑行為を受けているとか，財産的な被害を被ったなど，上記の不快感や不安を超える損害を被ったことについて主張，立証はない」として否定した。

21)　いわゆる早稲田大学江沢民講演会事件である。

った違法があるといわざるを得ない。」として，単に住所氏名程度だとしても精神的損害発生の可能性を十分に審理すべきとして，原判決を破棄し，差し戻した。

（2）差戻審：シンフォームの責任について

上記最判を受けた差戻審は，①シンフォームは業務用パソコンにスマートフォンを挿して充電することを認めていた，②シンフォームとしてMSC対応スマートフォンについては，個人情報不正取得の可能性を認識していた（そしてセキュリティソフトの導入・設定等対応もしていた），③必要な調査をすればMTP対応スマートフォンが流通していたことを認識できたというロジックで予見可能性を認め，シンフォームは少なくともAが機密性の高い個人情報であるデータベースを扱ってシステムを開発する業務を行っていたのであるから，同人がその私物のスマートフォン（外部記録媒体になり得る。）を持ち込むことを許してはならない義務があり，また，MTP対応スマートフォンに対する使用制御措置を講じる義務があった（もし，制御の結果業務に支障が生じるなら，スマートフォンを持ち込ませなければよかった）ところこれに違反したとした。

（3）差戻審：ベネッセの責任について

差戻審は，ベネッセについても，セキュリティソフトがMTP対応スマートフォンに対する書き出し制御機能等を備えているか否か，シンフォームの業務委託先の従業員が，ベネッセが管理する個人情報にアクセスすることができる業務用PCのUSBポートに個人の所有するスマートフォンを接続できる状況にあったかどうかについて適切に報告を求めていなかったことにおいて監督義務違反があったとした。

（4）差戻審：損害について

差戻審は，原告が親であり，原告自身の住所・氏名・電話番号はホームページなどで開示されていたことなど，本件に顕れた一切の事情を考慮すれば，慰謝料1000円を支払うべきものと認めるのが相当であるとした。

１３　これらの裁判例をどのように読むべきか

（1）時期ごとの変化

ベネッセ事件については，その裁判例を概ね3つの時期に分けることができる。平成30年6月20日以前（同日を含む），平成31年4月25日以前（同日を含

む）及びそれ以降（令和の裁判例）である。

平成 30 年 6 月 20 日以前において，裁判例は，損害を否定する傾向にあった。しかし，上記最判平成 29 年 10 月 23 日において，氏名，性別，生年月日，郵便番号，住所及び電話番号等であっても「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」ところ，名簿業者等への漏洩といった本件の事実関係によれば，プライバシーが侵害されたと言える以上，精神的損害の有無及びその程度等について十分に審理すべきであったと判示している。このような判示を経て，その後の裁判例，すなわち上記東京地判平成 30 年 12 月 27 日以降は，概ね損害賠償を認めるようになっている[22]。

その後の平成の時代には，シンフォームとベネッセが，書き出し制御措置を講じる等のなすべき注意を怠ったとして注意義務違反を認める裁判例と，シンフォームとベネッセはなすべき注意を怠ったとはいえないものの，A が使用者責任の意味におけるシンフォームの被用者であったとしてシンフォームに使用者責任のみを認める裁判例に分かれていた。

そして，令和時代には，全ての裁判例がシンフォームとベネッセの注意義務違反を肯定している（使用者責任については，これを明示的に否定するものと，使用者責任を論じるまでもないとするものの双方が存在する）。

（2）シンフォームの責任について

シンフォームの責任として，MTP スマートフォンを含めて書き出し制御措置を講ずべき注意義務を認めた裁判例が多い。具体的には，上記東京高判令和 3 年 5 月 27 日，上記京都地判令和 3 年 1 月 19 日，上記東京高判令和 2 年 3 月 25 日（双方），上記東京高判令和元年 6 月 27 日（原審：東京地判平成 30 年 6 月 20 日）及び上記大阪高判令和元年 11 月 20 日がこれを肯定した。セキュリティソフトの設定を見直し，これを適切な設定に変更すべき注意義務があったとする上記東京高判令和 3 年 3 月 17 日も同趣旨と思われる。

基本的には令和の時代においては，全ての裁判例がこの義務を認めているものの，それ以前には，この義務を否定する裁判例も多かった。例えば，上記千葉地判平成 30 年 6 月 20 日は「当時，書き出し制御システムを採用していない企業が過半であり，MTP スマートフォンへのデータの書き出しを防止するには，

22)　なお，2 つの東京地判平成 30 年 6 月 20 日は最判平成 29 年 10 月 23 日の後にもかかわらず，損害を否定している。しかし，これらの判断はいずれも控訴審において否定されている。

従来のスマートフォンとは異なる対策を講じる必要があるということが，一般的に認識されていなかった」等としてこの義務を否定していた。

この点は，「携帯電話端末における MTP 普及率についての調査報告」（例えば，上記東京高判令和元年 6 月 27 日（原審：東京地判平成 30 年 6 月 20 日）等が引用）によれば，平成 25 年 6 月時点で MTP 対応スマートフォンの普及率が約 7%と，必ずしも高いとはいえなかったことから，そのような普及率の高いとはいえない技術に対応する義務を認めることについて裁判所が当初は消極的だったものと思われる。これに対し，上記東京高判令和元年 6 月 27 日は，当時において MTP がどの程度普及していたか等についても，当該判示の後に（普及率が上記の認定を否定するものではないという程度の）検討はしているものの，そのような具体的検討をする前に「デバイスや OS は，バージョンアップにより高機能化していくものであるから，それに応じて，接続されるデバイスを制御してデータの漏えいを防いでいく必要がある」として，いわば最新の状況に常に対応すべきという抽象的一般論を提示している。このような判示は消費者にとってはありがたいものの，事業者の立場からすると，いわば「結果責任」を認めるに等しい判断ともいえる。むしろ，ベネッセ及びシンフォームが「事業活動上取り扱う対象は顧客からの大量の個人情報であり，情報管理に関する社会一般の認識に照らしても情報セキュリティ対策に細心の関心を払うべき立場にある」ことを強調した上記東京高判令和 3 年 3 月 17 日のような，具体的事情の下における厳格な情報管理の必要性を踏まえた判断の方を今後の他事件にも適用される一般論として理解すべきであろう[23]。

そして，上記東京高判令和 3 年 5 月 27 日，上記京都地判令和 3 年 1 月 19 日及び上記大阪高判令和元年 11 月 20 日は，これに加え，執務室内に私物のスマートフォンの持込みを禁止する措置を講ずべき注意義務も肯定している。上記大阪高判令和元年 11 月 20 日は，「オフィスであっても，通常業務が行われている場所だけとは限らず，本件の業務委託のように，専ら本件システム開発業務のために，サーバにアクセスして重要な情報に接続可能な状態で委託業務を遂行している場面においては，おのずからそのセキュリティ対策の程度に差異が生

23) とはいえ，常に最新状況に対応すべきといった判断が消費者側から引用されると思われるところ，事業者としては，裁判所がこのような判断を先例として理解する可能性にも留意が必要である。

じるのであって，A の担っていた本件システム開発業務は，サーバルーム内での業務と何ら遜色のないものであった」として，A が業務を行なっていた区画がサーバルームに準じることを理由としている（上記京都地判令和 3 年 1 月 19 日も同様である）。このような具体的な状況の認定に則した判断としては肯定し得るだろう[24]。

（3）ベネッセの責任について

上記の経済産業省の勧告において，ベネッセが，シンフォームに対して行う定期的な監査の際に本件データベースを監査の対象としていなかった等，委託先に対する必要かつ適切な監視を怠っていたことが個人情報保護法 22 条に違反すると指摘されていた。しかし，上記のとおり，個人情報保護法上の義務は公法上の義務に過ぎない。

令和の裁判例は，シンフォームによるセキュリティソフトの設定に関し，ベネッセの監督義務違反を認めている。しかし，委託者が，具体的に受託者におけるセキュリティソフトが MSC 方式のみならず MTP 方式に対応しているかを確認し，かつ，MTP 方式に対応していなければこれを変更するように指摘する義務を負うという結論を，ベネッセとシンフォームを離れた個人データの取扱いの委託に関する「一般論」としてみると，やや重すぎるきらいがある。とはいえ，ベネッセとシンフォームが同一グループに属する兄弟会社の関係にあり，通常よりも一段重い監督を求めるという観点は理解できなくもないだろう[25]。

（4）損害について

2 つの東京高判令和元年 6 月 27 日（2000 円）や，上記大阪高判令和元年 11 月 20 日（1000 円）のような判断もあるものの，最近の高裁レベルの判断は概ね慰謝料の額を 3000 円としている。

また，多くの地裁における敗訴事例は「本人訴訟」であるが，なぜ代理人をつけない/つけられないかといえば，弁護士費用相当額としてたとえば 3000 円の 10%として 300 円の賠償しか認められないからであるという点も指摘できるだ

---

24)　なお，上記東京高判令和 3 年 5 月 27 日は「シンフォームは，業務への支障を主張したが，個人情報の流失の危険に比して，執務室内での私物スマートフォンを使用することによる便宜が上回るような具体的な事情があったとも認められない」としており，リスクと便益の比較を想定しているところ，このようなリスクと便益を対比する思考方法そのものは正当であろう。この点については本稿Ⅲ5 も参照のこと。

25)　逆にいえば，このような具体的なセキュリティソフトの設定に関する監督まで必要であるという判示の射程もその範囲に留めるべきと思われる。

ろう。

この点については，ベネッセ事件のみに基づき判断をすべきではなく，他の情報漏洩事件の損害と比較すべきであり（Ⅳ・2 参照），また，情報漏洩事件によるプライバシー侵害のみならず，名誉毀損等も含む人格権侵害全体についてその損害賠償の水準や相応する弁護士費用の問題を考えるべきである[26]ものの，多くの高裁レベルの裁判例が現在の裁判所の「相場」を示したといえるベネッセ事件はそのような検討の際に参考になると思われる。

Ⅲ　セキュリティと責任分担・責任共有

1　責任分担・責任共有の重要性

現在においては各企業がセキュリティリスクに直面している。そして，全てのセキュリティリスクについて他社に「お任せ」できる訳ではなく，自社の負うべき責任の範囲と他社に負わせるべき責任の範囲を自社の認識においても，契約上の書面においても明確にし，セキュリティリスクを分担ないし共有していかなければならない。

この点については，例えば「クラウドサービス提供における情報セキュリティ対策ガイドライン」[27]22 頁において，「クラウドサービスの情報セキュリティを高めるためには，クラウドサービス事業者とクラウドサービス利用者が協力して，クラウドサービスに対する責任を共有する必要がある。この責任を共有するという考え方（責任共有モデル）を多くのクラウドサービス事業者が採用している。」とされているように，クラウドサービスの側面では議論が進んでいる[28]。しかし，クラウドサービス以外においてもこのような問題意識はあてはまるよ

---

26)　名誉毀損につき，松尾剛行・山田悠一郎『最新判例にみるインターネット上の名誉毀損の理論と実務』（勁草書房，第 2 版，2019 年）370 頁参照。

27)　「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）（案）」総務省 <https://www.soumu.go.jp/main_content/000760537.pdf>。

28)　松尾剛行『クラウド情報管理の法律実務』（弘文堂，初版，2016 年）71 頁以下も参照。また，「クラウドサービスのセキュリティは一般的に『責任共有モデル』が採用されており，クラウドサービス事業者と利用者・調達者の共通の認識の下，それぞれの管理権限に応じた責任分担を行うものである。そのため，クラウドサービス事業者と利用者・調達者は，それぞれの役割を適切に果たすことで，クラウドサービスに関するセキュリティリスクを最小化するために，共に協力することが望ましい。」とする「ICT サイバーセキュリティ総合対策 2021」サイバーセキュリティタスクフォース <https://www.soumu.go.jp/main_content/000761893.pdf> 25 頁も参照。

うに思われる。

そこで，複数の企業間で，どの企業がどこまでの範囲についてセキュリティに関する責任を負うべきかが問題となった裁判例を検討したい。

２　決済に関する事例

(1) はじめに

決済に関する事例では，クレジットカード決済等における不正使用等や情報漏洩が生じた場合において，その責任をどの当事者が負うべきかが問題となるものが見られる。

(2) 裁判例

東京地判平成 25 年 3 月 19 日第一法規 29024625[29]は，クレジットカード決済代行サービス会社（原告）が，原告と契約していたクーポン共同購入サイト（本件サイト）運営企業（被告）に対し，被告がなすべき義務を怠った結果，クレジットカード情報が漏洩したとして原告が被った損害の賠償を請求した事案である。裁判所は，被告がアクセスログを残すように設定していなかったため，いかなる経緯でクレジットカード情報が漏えいしたのかについては明らかになっていないとしたものの，被告の多数の顧客のクレジットカード情報が漏えいしていること等に鑑みると，本件サイトに何らかの不正なアクセス等が行われることによって被告の顧客のクレジットカード情報が漏えいしたことが推認されるとした。その上で，原被告間の契約上，被告は会員のカード情報等を第三者に閲覧等されないように本件サイトを適切に管理する義務を負っていたと認定し，かかる義務への違反を認めた。

東京地判平成 26 年 5 月 14 日第一法規 29041198 は，オンラインショップ開設者（原告）とシステム開発業者（被告）の間で，原告のオンラインショップにおいてクレジットカードが不正使用されたことから，原告が被告に損害賠償を求めた事案である。両当事者間でオンラインショップシステムの利用に関する契約が締結されたところ，当初は，3D セキュアという本人認証オプションが採用され，非対応カードの場合に決済ができないようにしていた。しかし，特定の顧客が非対応カードを用いて決済を試み，決済ができなかったため，原告に対して

29)　吉本・前掲注 7）351 頁以下において事例 40 として取り上げられている。

問い合わせを行なった。原告は被告に対し，当該顧客に対応するようにとの連絡し，被告は，当該顧客については，3D セキュア非対応カードであったため決済ができなかったこと，そのため，3D セキュア非対応カードでも決済が通るように設定変更をしたことを報告し，元のように 3D セキュア非対応カードは決済を通さない設定に戻す必要があれば連絡するように記載したメールを送信した。上記不正使用は，3D セキュア非対応カードによるものであった。裁判所は，被告は，原告の指示に従った対応を取り，その旨を原告に報告していたものということができ，仮に，被告が，上記作業につき何らかの義務を負っているとしてもその義務違反が存在するということはできないとした。なお，本判決については，本稿 4（4）も参照。

上記東京地判平成 30 年 3 月 29 日第一法規 29049388 は，原告が決済代行を含むネットショップ開設サービスを提供しており，被告がかかるサービスを利用して通信販売事業を営んでいたところ，被告の通信販売事業にかかる一部の代金がクレジットカードの不正使用により決済された疑いがあるとして，原告が被告に対し，契約に基づき不正使用にかかる代金等の支払いを求めた事案である。被告は，原告の決済サービスのセキュリティに問題があったにもかかわらず，不正使用にかかるリスクを被告に転嫁するべきではないと主張した。裁判所は，原告がセキュリティコードの入力をさせるシステムを整備した上で，クレジットカードの不正利用の疑いがある取引について情報を入手し次第，これを被告に伝えて，契約解除及び商品発送の取りやめを勧奨する等一定の措置を行なっていると認定した。そして，原告の決済手数料が非常に安く，決済を運営すること自体による利益は決済額の 0.06 パーセント余りにとどまることを考慮すれば，3D セキュアによる本人確認等を実施する等の被告の主張する措置を講じていなくても，原告の権利行使を法的に制限するような特段の事情があるとはいえないとした[30]。

（3）検討

まず，東京地判平成 25 年 3 月 19 日の事案は，被告はログすら取っていないため，具体的にどのような態様でカード情報が漏洩したかが不明な事案である。

---

30) その他，長男によるカード利用について，カード会社が 3D セキュア等の十分なセキュリティ措置を講じていないから支払う必要がないという主張に対し，カード会社が一定の本人確認をしており，このような確認を超えた不正利用防止措置等をしなければならないとする根拠を見出すことはできないとした東京地判平成 28 年 5 月 17 日第一法規 29018477 等も参照

何が起こったかを確認する上でもログを取ることは重要であり，その意味で，被告がカード情報保護義務を果たしていないという判断はやむを得ないところである。

次に，上記東京地判平成 26 年 5 月 14 日においては，結果的には，3D セキュア非対応カードも決済を通す設定にしたことによって，不正使用が生じた可能性が高いところ，かかる設定変更は直接的には被告（システム開発業者）が実施したものである。しかし，それはユーザ企業である原告の要求（3D セキュア非対応カードの顧客に対応せよ）に応じた結果であり，被告としてなすべき報告（本稿 4 (4) も参照）を行なっていた。そのような状況において，責任は原告にあるとされた。本判決はユーザ企業が誤った（又はリスクのある）指示をシステム開発業者に出せば，その結果として誤った結果が生じにてもユーザの責任となり得ることを示唆している。

更に，上記東京地判平成 30 年 3 月 29 日は基本的には，カードが不正使用された場合に，通信販売業者（被告）と決済代行業者（原告）のいずれが責任を負うかについて，決済代行業者が一定のセキュリティに関する対応を行なっている前提の下では，契約どおりその責任を通信販売業者に負わせることができるという判断をしたものと理解されるだろう（本稿 5 も参照）。

３　プラットフォーム等第三者が介在する場合の事例

(1) はじめに

近年では，プラットフォーム等の第三者が関与し，その前提での責任が問題となる。

(2) プラットフォームに関する裁判例

プラットフォーム自身の詐欺防止に関する責任が問題となったものとしては少し古いものの名古屋高判平成 20 年 11 月 11 日自保ジャーナル 1840 号 160 頁が存在する。同判決は，「利用契約における信義則上，被告（注：プラットフォーム事業者）は原告ら（注：詐欺被害者）を含む利用者に対して，欠陥のないシステムを構築して本件サービス（注：インターネットオークションサービス）を提供すべき義務を負っているというべき」とした上で，「被告が負う欠陥のないシステムを構築して本件サービスを提供すべき義務の具体的内容は，そのサービス提供当時におけるインターネットオークションを巡る社会情勢，関連法規，システムの技

術水準，システムの構築及び維持管理に要する費用，システム導入による効果，システム利用者の利便性等を総合考慮して判断されるべき」として，当該事案において結論としてプラットフォームの責任を否定した原審（名古屋地判平成 20 年 3 月 28 日判例時報 2029 号 89 頁，判例タイムズ 1293 号 172 頁）の判断を是認している。

東京地判平成 27 年 2 月 25 日第一法規 29028813 は，ユーザである原告が SEO 対策業者である被告に検索順位向上等を内容とする SEO 対策を依頼したが，順位がむしろ低下したとして錯誤等を主張した事案である。この事案では，結果的に順位は下がったものの，一時は検索結果の表示順位が 2 位にまで向上していたことや，その後 Google 社が検索順位決定の仕組み（アルゴリズム）の変更を行ったことも認定されている。裁判所は，被告の実施した SEO 対策は，一定の有用性があったというべきで，原告において錯誤があったと認めることはできないとされた。

東京地判平成 30 年 12 月 27 日第一法規 29051418 は，ユーザ企業が IT 業者に依頼して，民泊プラットフォーム上でのユーザ企業の物件の管理をさせていたところ，突然民泊プラットフォーム上での物件の閲覧が不能となったという事案における IT 業者の責任が問題となった。裁判所は，プラットフォームが「我々は最近，誰かが自分のアカウントへの不正な変更を加えている可能性があることを検出しました。このため，あなたのＥ（注：プラットフォーム）のパスワードがリセットされており，我々はあなたのアカウントを保護し，それへのアクセスを取り戻すためにいくつかの追加のセキュリティ機能を有効にしています。」等というメールを送付していること等を踏まえ，閲覧不能状態は，IT 業者のアカウントの管理の不備にあることを認めるに足りる証拠はなく，（プラットフォーム側のセキュリティ上の対応等の）IT 業者の責めに帰すべからざる事由により発生したものと認めるのが相当であるとした。

（3）プラットフォーム以外の第三者

東京地判令和元年 12 月 20 日第一法規 28280353 では，ユーザ企業がシステム開発業者に通販サイト用ソフトウェアのカスタマイズ及びサイトの運用，保守管理を依頼した。ところで，ここで利用される通販サイト用ソフトウェアは，OpenSSL と言われる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を利用していた。そして，その OpenSSL の脆弱性によりトラブルが生じてしまった。裁判所は，契約書上の「サイトの運用，保守管理」との記

載は，必ずしも通販サイト用ソフトウェアが利用する暗号化通信ソフトウェアを含む全体を意味しないし，契約書上の通販サイト用ソフトウェアの「カスタマイズ」という記載も，当該通販サイトにおいてOpenSSLを経由した通信がされるからといってカスタマイズ業務の委託を受けた者が，当然にOpenSSL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としてシステム開発業者の責任を否定した。要するに，システム開発業者は，OpenSSLに関するセキュリティ対策をその役割として担っていない以上，OpenSSLの脆弱性を発見，指摘，回避，是正等する義務を負わず，その結果，OpenSSLの脆弱性によるトラブルは，システム開発業者の責任ではない（ユーザ企業の責任である）と判断されたのである。

東京地判平成25年11月28日第一法規29030809は，ユーザである原告がシステム開発業者である被告との間でウェブサイト等を構築・管理する契約を結んでいたところ，被告がレンタルしていたサーバの期限を切らしてしまい，ドメインが失効し，ウェブサイトが利用できなくなった事案であり，裁判所はシステム開発業者である被告に責任があるとした。

東京地判平成30年1月22日第一法規29048682は，被告のゲームアプリケーションがダウンロードされるよう，原告が広告施策を講じることを内容とする契約が締結され，原告が当該契約に基づき報酬を請求した事案である。この広告施策においては，リワード広告といって，特定のアプリケーションをダウンロードすると，ユーザがポイント等の報酬を得ることができる施策が選択された。被告は，ユーザが，リワードを目的として機械的にIPアドレスを変更する等して機械的に報酬の条件である5万ダウンロードを達成した外観を作出したと主張した。裁判所は，リワードを目的とするユーザが機械的にIPアドレスを変更するなどして，二重，三重にポイントの獲得を目的とする行為まで明確に排除されているとはいえず，そのような意味での機械的操作自体は許容されているものと解さざるを得ないとし，報酬請求を認容した。

（4）検討

プラットフォーム事業者として一定の詐欺等の防止に関する（セキュリティに関する）義務を負うことを認定した上記名古屋高判平成20年11月11日は，今後のプラットフォームの責任を論じる上でも重要である。もっとも，具体的にどの程度の義務を負うのかという一番重要な点に関する判断基準が総合考慮である

ため，判断・予測しにくいという批判は可能であろう（5 も参照）。

上記東京地判平成 27 年 2 月 25 日及び上記東京地判平成 30 年 12 月 27 日はそれぞれプラットフォーム側の対応により，アルゴリズム変更やアカウント停止等がなされ，その結果として業者側として意図した結果（検索順位の上昇や物件の管理）を実現することができなかったものの，業者の責任ではないとされたものである。プラットフォームが重要性を増すにつれ，このような紛争も増加すると思われるが，その際にこれらの裁判例の判断が参考となるだろう。

上記東京地判令和元年 12 月 20 日はオープンソースソフトウェアの脆弱性の問題について，当該案件においてはシステム開発業者の業務内容に含まれていないと解釈された事案と理解される。これに対し，上記東京地判平成 25 年 11 月 28 日の事案では，ユーザである原告は，自らサーバを管理するだけの知識を持ち合わせていないと認定されており，ドメインの維持・管理が契約内容に含まれていたと認定され，その結果，システム開発業者が責任を負うとされた。

上記東京地判平成 30 年 1 月 22 日は，介在する「第三者」というのが個人ユーザ（ゲームアプリケーションをダウンロードする人）であるという特殊性があるところ，具体的な事情の下，そのような者による，ある意味では「不正」とも評し得る機械的操作が一定数実施され得ることが，当事者間の合意上明確に排除されていないと判断したものである。ユーザ企業としては，このような場合の報酬請求を防止したければ，契約上明確に機械的操作によるダウンロード数を除外する旨合意する必要があるといえよう。

4　システム開発に関する事案

(1) はじめに

最後に，システム開発に関する事案で，ユーザ企業とシステム開発業者の間のサイバーセキュリティに関する責任の分担が問題となったものを紹介したい。

(2) 仕様が特定されている場合

請負契約を想定すると，システムの要件・仕様は（必要に応じてシステム開発業者の支援の下で）ユーザが決定し，それに基づき請負人たるシステム開発業者が「仕事」たるシステムを完成させるのが原則である。そこで，サイバーセキュリティに関するトラブルが生じた場合のベンダの責任については，基本的には，どのよ

うな要件・仕様が合意されたのか（構築されたシステムの要件・仕様は合意どおりか）によって判断される。そして，実務上，仕様書等に基づき要件・仕様が認定されることが多い。よって，仕様書にセキュリティ要件が明記されていれば，それが完成すべき「仕事」となる[31]。

SQL インジェクションという不正対策を実施すべきことが仕様上明記されていた事案においてSQLインジェクション対策を怠ったとして損害賠償を認めた東京地判平成30年10月26日第一法規29052102は，このような点を明示した裁判例と言える。

（3）仕様が特定されていない場合

しかし，問題は，セキュリティ要件が仕様書等に明示されていない場合である。

東京地判平成26年1月23日判例時報2221号71頁は，当時のIPAの公表内容等から，SQL インジェクション対策については仕様書上明記されていなくともその対策がベンダの義務の内容となるとした[32]。

確かに，ユーザとして，仕様書に何も書いていなければシステム開発業者に対し一切のセキュリティ対策を求めることができない訳ではない，という意味で，この裁判例の判断は，ユーザに有利である。しかし，それは決して，システム開発業者が何もないところから無限の責任を負うという意味ではなく，あくまでも，その時点で知られている脆弱性の内容及びその重大性に鑑みて，流石に専門家として何の合意がなくても対策をすべきとされるいわば「最低限」の部分について黙示の義務があるとされるに過ぎない。そこで，ユーザとしても，この黙示のセキュリティ要件が認定された裁判例に依拠することなく，自らセキュリティ要件を明示的に合意するよう努力すべきである[33]。

（4）説明義務

セキュリティについてはユーザに専門知識がないことが多いため，システム

---

31)　この点は，松尾剛行・西村友海『紛争解決のためのシステム開発法務―AI・アジャイル・パッケージ開発等のトラブル対応』（法律文化社，2021年刊行予定）及び「『情報システム・モデル取引・契約書』第二版」独立行政法人情報処理推進機構社会基盤センター<https://www.ipa.go.jp/ikc/reports/20201222.html> 20頁以下参照。

32)　「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。」

33)　そして，独立行政法人情報処理推進機構社会基盤センター・前掲注31）もそのような仕様書におけるセキュリティ要件の明記を推奨し，セキュリティ基準の準用等の実務的な対応を紹介している。

開発業者が説明をすべきだ，という趣旨の説明義務違反の主張がされることがある。

東京地判平成 25 年 11 月 19 日第一法規 29030801 は，セキュリティに関する説明義務違反を認めたものである。この事案では，システム開発業者である原告が開発したシステムが，FTP サーバへの接続を要する仕様であったところ，利用者によってはセキュリティの関係で FTP サーバへは接続できない設定を採用していることが予想されることから，ユーザである被告として，利用者に FTP サーバへの接続を制限する旨のセキュリティ上の設定を解除してもらう必要があるという難点を有するものであった。裁判所は「システム開発において FTP サーバを利用する内容とすることが直ちに債務不履行に当たるものではないが，FTP サーバの上記のような特性から，FTP サーバを利用する内容のシステムとすることでシステムの運営上不都合が予想されるような場合には，開発段階においてこれを説明する義務があった」として原告が説明義務を負っているところ，これに違反したとした。

しかし，裁判所は，決済に関する上記東京地判平成 26 年 5 月 14 日（上記 2 (2) 参照）において，システム開発業者の説明義務等を限定している。すなわち，上記事案では，説明義務違反も問題となっており，ユーザ企業である原告は，被告であるシステム開発業者が，3D セキュア非対応のカードも通すような変更をすれば不正使用事件が発生してしまう旨を説明する義務を負うと主張したが，裁判所は，被告であるシステム開発業者は，原告の指示に従った対応を取り，その旨を原告に報告していたとして説明義務等の義務を負わないとした。

ユーザが主導的に対応を求めた上記東京地判平成 26 年 5 月 14 日と，そうではない上記東京地判平成 25 年 11 月 19 日の違いという説明も可能であるが，今後関係するより多くの裁判例が蓄積することを期待したいところである。

(5) リモートアクセス

なお，現在の新型コロナウイルス禍では，リモートアクセスよるシステム開発について注目が集まっている。

東京地判平成 25 年 11 月 27 日第一法規 29026549 は，システム開発業者が，不具合の原因が早期に特定できなかった原因について，ユーザがリモートアクセスを承認しなかったためであったと主張した。しかし，契約上，リモートアクセスを利用することはユーザの義務ではなく，また，リモートアクセスを承認す

ることによって，システム開発業者がページ不表示エラーの原因を解明することができ，この修正作業を完遂することができたといえる客観的な証拠はないとした。この事案は，要するに，ユーザがリモートアクセスを承認してもしなくてもいずれにせよ不具合を修正できないとして，ユーザがリモートアクセスを承認しないことに問題がないとされた事案である。

これに対し，東京地判平成 30 年 10 月 19 日第一法規 29051931 は，ユーザ企業である原告がシステム開発業者である被告に映像配信等を内容とするシステムの構築を依頼した事案において，ユーザ企業である原告が，リモート保守がなされたことに不満を述べた事案である。構築されたシステムについて，原告が多くの不満を主張したところ，その 1 つに，システム開発業者である被告の社屋から保守をするリモート保守を前提としたシステムとなっており，オンサイト保守（サーバ監視装置を原告の施設内に設置し，不具合が生じた場合の対応は技術者が現場に臨場して行う方式）を前提としていないという点が含まれていた。裁判所は，被告が，原告に対し，資料に基づき，サーバ監視保守システムの在り方についてリモート保守やオンサイト保守を含めた複数の選択肢を説明したこと，被告が原告の要望に応じてオンサイト保守のシステムを構築する場合には約 1900 万円の費用を要する旨の見積書を提出したところ，原告からその諾否の回答はなかったため，被告はリモート保守を前提としてシステムを構築したことを認定し，原告が被告の提出したオンサイト保守の見積りに応諾しなかったことから，オンサイト保守とすることの合意が成立しなかったことによるのであって，オンサイト保守に対応していないことをもって本件システムの重大な欠陥等には該当しないとした。要するにリモート保守であっても，システム開発業者側に何ら問題がないと判断したのである。

リモートアクセスについては，少なくとも Before コロナの時代においては両当事者間で特段の合意がなくても，当然に認められるという性質のものではなく，両当事者で合意をして行なっていくべきこととされ，合意の際には費用負担の問題も踏まえて（上記東京地判平成 30 年 10 月 19 日参照）決定されるべきと言えるだろう。今後の With コロナ時代においてはそれが変化する可能性はあるものの，少なくとも合意なきリモートアクセスによるセキュリティ水準低下を懸念する観点からは，従前と同様にセキュリティ水準を維持する方策や費用等について協議をした上で両当事者で合意をして行なっていくべきことに変わりないとも

思われる。

５　小括

上記の裁判例を踏まえると，決済やプラットフォームが介在する事案等，いわゆるクラウド以外の分野においても，責任分担・責任共有の考え方によって説明可能な裁判例が多く出現していると言えるだろう。具体的にその当事者の責任分担の範囲にはないと判断された事例においては，法的には，義務がない（上記東京地判令和元年 12 月 20 日等），帰責性がない（上記東京地判平成 30 年 12 月 27 日等），報酬請求の認容（上記東京地判平成 30 年 1 月 22 日等）等の形で処理されることになる。

加えて，決済に関する上記東京地判平成 30 年 3 月 29 日や，プラットフォームに関する上記名古屋高判平成 20 年 11 月 11 日は求められるセキュリティのレベルを判断する上で費用を考慮すると明言している（リモート保守に関する上記東京地判平成 30 年 10 月 19 日も参照）。サイバーセキュリティに関しては費用を無限にかけることができれば，いくらでもセキュリティのレベルを強化することが可能であるものの，現実には掛けられる費用には限界がある。そこで，サイバーセキュリティ対策費用対効果を考えながら優先度を考えて予算を確保し進めていくべきとされている[34]。そして，上術のような裁判例が出ているということは，このように，裁判所においても，費用対効果の概念をサイバーセキュリティ対策においても認める傾向が強まっていることの反映と言えるだろう。そこで，裁判所が求められるセキュリティに関してそのような費用の点を考慮して認定していることは，実務に正しい影響を与えると期待される[35]。

Ⅳ　CIA ごとの検討

１　情報セキュリティの CIA

情報セキュリティに関しては CIA という概念が有名である。すなわち，

---

34)　「サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集」20 頁 IPA < https://www.ipa.go.jp/files/000072309.pdf>参照。

35)　なお，関連して，ベネッセ事件に関する上記東京高判令和 3 年 5 月 27 日（上記Ⅱ4(1)参照）がセキュリティ対策を講じないことで増大するリスクと，セキュリティ対策を講じないことで得られる便益の比較を行っていることも参考になる。

・機密性（Confidentiality）―情報へのアクセスを認められた者だけがその情報にアクセスできる状態を確保することであり，第三者のアクセスによる情報漏洩事故が起こらないようにすることが例示される。
・完全性（Integrity）―情報が破壊，改竄又は消去されていない状態を確保することであり，データ消失事故や改竄被害等が発生しないようにすることが例示される。
・可用性（Availability）―情報へのアクセスを認められた者が，必要な時に，中断することなく，情報及び関連資産にアクセスできる状態を確保することである[36]。

以下では，サイバーセキュリティに関する裁判例についてCIA[37]ごとに検討していきたい。

２　情報漏洩等機密性が問題となった事案

（1）機密性侵害が問題となったものの違法性が否定された事案

機密性侵害が問題となったものの違法性が否定された事案の多くは，本稿が対象としないオフラインの事案，例えば，監視カメラによる撮影が受忍限度内等として正当とされた事案である[38]。その中で，Googleストリートビューによる洗濯物の公道からの撮影及び公表が非侵害とされた福岡高判平成24年7月13日判例時報2234号44頁（原審：福岡地判平成23年3月16日第一法規28170964。最決平成26年3月4日第一法規28270813で上告棄却，上告受理申立につき不受理となっている。）は，数少ないオンライン上の事案と言えるだろう。

（2）機密性侵害により賠償すべき慰謝料が問題となった事案

オンライン上の機密性侵害事案，とりわけ情報漏洩事案においては，多くの場合，責任が肯定されることを前提に賠償額が問題となっている[39]。

筆者が知る限り漏洩で最大の賠償を命じられたのは，1人あたり最大500万円の慰謝料が命じられた東京高判平成27年4月14日第一法規28231753（警視庁国

---

36)　松尾ほか・前掲注28）24頁。
37)　ただし，単純に開発したシステムにおいてシステム障害が発生したというだけに過ぎない事案はあえて除外している。システム障害等のシステム開発については，松尾ほか・前掲注28）参照。
38)　具体的な裁判例につき，松尾・前掲注13）73-74頁参照。
39)　なお，ここでは加害者が意図的に被害者の情報をインターネット上の例えばSNSや掲示板に書き込むといった類型を検討対象としていない。このような類型の具体的な裁判例につき，松尾・前掲注13）226-236頁参照。

際テロ捜査情報流出事件）である[40]。

これに対し，エステサロンに登録した情報の漏洩について 1 人当たり 3 万円の慰謝料を認めた事案（東京高判平成 19 年 8 月 28 日判例タイムズ 1264 号 299 頁），住民基本台帳データがシステム開発業務の再々委託先のアルバイト従業員により不正コピーされたことにつき 1 人あたり慰謝料 1 万円を認めた事案（大阪高判平成 13 年 12 月 25 日判例地方自治 265 号 11 頁），インターネット接続事業者の情報漏洩について 1 人あたり 5000 円の慰謝料を認めた事案（大阪高判平成 19 年 6 月 21 日第一法規 28142194）等，比較的低額の裁判例も多い。上記Ⅱで検討したベネッセ事件の慰謝料もこのような比較的低額の類型に属すると言える。

基本的には，これらの相違は流出したデータの性質によって説明されるだろう。警視庁国際テロ捜査情報流出事件では，単にイスラム教徒であるというだけでテロリストと目されてその宗教活動等を含む私生活を詳細に記録されたものであり，そのような性質に鑑みて高額の慰謝料が認められたものと思われる。

なお，興味深いものとして，従業員が業務上のデータが記録された USB ファイルを紛失した事案についてその内容が不明であり，流出したかも不明であるという状況の下，将来的な流出の危険性にさらされているという無形の損害を被ったとして 30 万円の損害賠償を認めた[41]東京地判平成 24 年 3 月 27 日労働判例 1053 号 64 頁（霞アカウンティング事件）がある。実務上は，流出したかもしれないものの，「流出した」という確証も「流出していない」という確証もないという，当該事案と類似する事案が相当程度存在すると思われ，そのような場合の一つの解決指針となり得るだろう。

（3）漏洩と債務の本旨

興味深い類型として，業務委託の際に，受託者が情報漏洩をしたことが債務の本旨に反するとして報酬請求権が否定されるのではないかが問題となった類型がある。

---

40) なお，福岡高判平成 24 年 7 月 12 日第一法規 28181607 はオフラインであるが，医療情報漏洩につき，100 万円の慰謝料を認めている。HIV 陽性である旨の情報の漏洩につき 200 万円を認めた福岡地久留米支判平成 26 年 8 月 8 日判例時報 2239 号 88 頁（ただし控訴審の福岡高判平成 27 年 1 月 29 日判例時報 2251 号 57 頁で 50 万円に減額）も参照。

41) 「上記 USB メモリに記録されていたデータの内容は証拠上不明である上，それが流出したか否かも不明であるが，このことをもって，被告会社が損害額の立証を尽くしていないと評価するのは相当ではない。このような点からすれば，現時点においては，将来的な流出の危険性にさらされるという被告会社のリスクを無形の損害として評価する他はないところ，諸般の事情を考慮すれば，上記紛失による被告会社の損害は，USB メモリ自体の価額も含めて，30 万円と認めるのが相当である。」

東京地判平成31年3月28日第一法規29054774では，ダイレクトメール運送の委託者と受託者の間で，受託者（の再委託先）が，宛名ラベルを上下二重に張り合わせるミスをし，その結果，顧客の氏名及び住所の一部が第三者である他の顧客に漏洩した。そして委託者は，かかる漏洩事故の発生を理由として，受託者の報酬請求を拒んだ。裁判所は，確かにダイレクトメール運送委託契約の付随義務として情報を漏洩しない義務があり，受託者において付随義務違反自体は存在すると認定した。しかし，委託者が顧客に対し，謝罪文書を発送するとともに，コールセンターを設置し，その費用を受託者に請求し，受託者はこれを支払っており，付随義務違反の債務不履行自体は解消されたものというべきであるとした。よって委託者は委託料債権の支払い義務を負うとしたものの，委託者はこの事故で信用を失い，ダイレクトメール印刷・発送等の業務の停止等の損害を被ったとして相殺を行なった。

債務者が付随義務の履行を怠ったに過ぎない場合につき特段の事情が存しない限り債権者は当該契約を解除できないとする古い最高裁判例（最判昭和36年11月21日民集15巻10号2507頁等）に鑑みると，それが単なる付随義務違反に過ぎないとされる限り，（相殺の主張はともかく，）債務不履行が解消されるまで支払いを拒むことができるのか疑問があるものの，一つの事例として参考になる[42]。

３　データ消失・改ざん等完全性が問題となった事案

（1）はじめに

データが消失したり改ざんされたりした場合においては，まずはその原因が問題となる。その上で，データ消失や改ざんについてある当事者が責任を負うとされた場合，データの価値その他の損害が問題となる。ただし，多くのデータ消失の事案においてはバックアップを適切に取得しておくことで，データ消失が発生してもその損害を最小化できることから，バックアップ取得義務も問題となる。

---

42)　なお，東京地判平成25年3月22日第一法規29025954及び平成27年10月14日第一法規29014550も参照。参考まで，漏洩による事業上の損害が問題となったものとして東京地判平成31年1月30日第一法規29052637がある。

（2）データ消失に関する責任

東京地判平成 29 年 3 月 2 日第一法規 29046608 は，個人ユーザである原告が，サポートサービスを提供するパソコン製造企業である被告による遠隔でのサポートを受けた際に，原告のパソコン上のデータが消失したという事案である。裁判所は，コンピュータ機器の操作において偶発的にデータが消失するリスクは常に存在していること，及び，被告が規約上購入者に対しバックアップコピーの作成を求めているとした上で，バックアップ作成を怠ったことによりデータ消失が生じたとしても，特段の事情がない限り，購入者の責に帰されるべきものというべきであるとして被告に責任はないとした。

東京地判平成 27 年 5 月 22 日第一法規 29022240 は，パソコンのハードディスク上のデータ消失事案である。裁判所は，ハードディスクドライブに異常が生じ，データが消失する事態は一般的に想定されているといえ，取扱説明書にも，ハードディスクの不具合によりデータ消失の危険があることから，バックアップをとるように注意喚起する記載があるとした上で，顧客が通常の使用方法により 3 年間パソコンを使用していたという事実が認められるとしても，パソコンに欠陥があったことの主張立証責任が製造業者側に転換されることはないとし，欠陥の立証がないとした。

これらの裁判例は，論理は異なるものの，現代の電子機器は何らかの原因でデータが消失する可能性を常にはらんでおり，だからこそバックアップが必要であるという常識を踏まえ，責任論の判断に生かしたものと言えるだろう[43]。

なお，やや特殊な事案として東京高判平成 30 年 12 月 20 日第一法規 28270319 は，医療事故訴訟に関係して，初診時に入力したデータが保存されていなかった原因は必ずしも明らかではないところ，あらゆるデータ消失の原因を考慮して万全の対策を執らなければタブレット端末の使用をしてはならないという注意義務を医療機関が負うとは認められないとした。この点は，データ消失のリスクがあるからといって新たなテクノロジーを導入してはいけないとはいえないことを示したという点で，裁判所が新たなテクノロジーの導入を後押しする判示をしたものと読むこともできるかもしれない。

---

43) その他，東京地判平成 28 年 3 月 3 日第一法規 29017679，東京地判平成 31 年 3 月 19 日第一法規 29054334，東京地判平成 21 年 8 月 7 日第一法規 28173389 等も参照。

(3) データの価値及びバックアップ

では，データ消失の場合の損害額はどのように計算されるのだろうか[44]。

まず，再作成費用がデータの価値とされることが多い。

東京地判平成 25 年 3 月 13 日第一法規 29027407 は SEO 業者がアクセス解析ツールのアカウントを削除したことで，ユーザ企業に損害が発生したとしたものの，業者に委託すれば，再作成費用は 6 万 7200 円で済むとして 6 万 7200 円の損害賠償請求のみを認めた[45]。

また，復旧費用も認められることがある。

東京地判平成 25 年 11 月 14 日第一法規 29030752 は，退職者が退職の際にデータを消去したという事案において，会社は得べかりし利益を失ったと認めることはできないものの，他の従業員が，削除したデータを調査し，復元するために，勤務時間を費やしたことについて，調査や復元のための費用は，退職者の行為と相当因果関係のある費用と認められるとした[46]。

特殊な事案であるが，東京地判平成 25 年 11 月 26 日第一法規 29031125 は，元理事によるサーバ破壊につき，サーバ復旧費用約 350 万円を損害として認めた。

更に，慰謝料を認める裁判例もある。

東京地判令和 2 年 9 月 17 日第一法規 29061107 は，テレビ受像機の買取りの依頼を受け電気店の被告がテレビに接続されていたブルーレイディスクレコーダーのケーブルを外してテレビを運搬しようとしたところ，その操作を誤り，レコーダー内に記録されていた映像データを全て消去してしまったという事案である。裁判所は，顧客の精神的苦痛を慰謝するに足りる金額としては，45 万円が相当であるとしたが，バックアップを怠ったというのは顧客の過失であったというほかないとし，過失相殺によって 20％を減額した[47]。

---

44) なお，損害の否定例に東京地判平成 18 年 6 月 30 日判例時報 1959 号 73 頁がある。

45) その他，神戸地判平成 2 年 7 月 24 日判タ 743 号 204 頁，大阪地判平成 9 年 9 月 18 日判タ 992 号 166 頁，旭川地判平成 11 年 6 月 30 日交通事故民事裁判例集 32 巻 3 号 975 頁，東京地判平成 13 年 9 月 28 日裁判所 HP，東京地判平成 16 年 32 日判例秘書 L05930927，岡山地判平成 14 年 11 月 12 日裁判 HP，東京地判平成 15 年 3 月 14 日判例秘書 L05831097 等も参照。

46) その他，東京地判平成 17 年 10 月 27 日交通事故民事裁判例集 38 巻 5 号 1455 頁，東京地判平成 18 年 531 日判例秘書 L06132208，東京地判平成 20 年 9 月 8 日 Westlaw2008WLJPCA09088002，東京地判平成 23 年 4 月 15 日 Westlaw2011WLJPCA04158001，東京地判平成 25 年 11 月 26 日 Westlaw2013WLJP CA11268014，東京地判平成 25 年 11 月 14 日 Westlaw2013WLJPCA11148002 等も参照。

47) その他，広島地判平成 11 年 2 月 24 日判タ 1023 号 212 頁，上記岡山地判平成 14 年 11 月 12 日，上記東京地判平成 15 年 3 月 14 日等も参照。

（4）改ざん

東京地判平成 30 年 3 月 16 日第一法規 29049333 は，インターネット上の株式取引に関する証券会社と顧客間の紛争において，アクセスログが改ざんされた等と顧客は主張したが，原データに人為的な編集や改ざんがなされた形跡はうかがうことができない等とし，アクセスログの内容が虚偽であると認めることはできないとした。

東京高判平成 31 年 4 月 11 日第一法規 28272501 は，オンライン上の改ざんではないが，中古車のメーター巻き戻しという改ざんを理由とした会員登録抹消処分を有効とした。

なお，ゲームアプリケーションのダウンロードに関する上記東京地判平成 30 年 1 月 22 日は，ダウンロード回数の改ざんの事案と理解することも可能であろう。

４　システム障害等可用性が問題となった事案

東京高判平成 22 年 3 月 25 日第一法規 28161488 は，航空券を購入した消費者が予約チェックインシステムの障害のため，定刻通りに到着できなかったことについて，航空会社に対し損害賠償を請求した事案であるが，システム障害発生につき過失はない[48]等として債務不履行はないとした。

しかし，東京高判平成 25 年 7 月 24 日判例時報 2198 号 27 頁は，みずほ証券が，株式誤発注事件に際し，東証のシステムに障害がなく，適切に取消処理をすることができていれば，損害が発生・拡大しなかったと主張した。裁判所は，東証に適切に取消処理ができるコンピュータ・システム提供義務の不履行が認められるものの，重過失であるとはいえず，免責規定により免責されるとした[49]。

システム障害に関するユーザ企業側のテスト等によりシステム障害の原因をあらかじめ特定し，除去することに関する責任について，上記東京高判平成 25 年 7 月 24 日は上記東京高判平成 22 年 3 月 25 日よりも重く考えているように思

48)　「控訴人らは，本件システム障害の原因の特定は容易で，被控訴人は既に改善していることからすれば，本件システム障害の発生という結果の予見が可能であったと主張する。しかしながら，発生した後に本件システム障害の原因を分析し，それに対処する方法を考え出すことができたことから，発生前にシステム障害を予見してこれが発生しないように対処することが可能であったということはできず，これが極めて困難であったことは，引用した原判決記載のとおりである。」

49)　なお，別の争点である，売買停止義務違反については重過失ありとされている。

われる。

なお，東京地判平成 26 年 2 月 18 日第一法規 29039636 は，セキュリティソフトによりパソコンが操作できなくなる事象について，ソフトを現状のままで使用許諾し，どのようなパソコン環境の下でも正常に作動することを保証するものではないという文言どおりの免責を認めた。上記東京高判平成 25 年 7 月 24 日でも免責規定が適用されているところ，このような可用性の問題となった事案については免責規定が問題となることが多いと言えよう。

V　おわりに

本稿は，2020 年 10 月 3 日のサイバーセキュリティ法制学会第 9 回研究会における「サイバーセキュリティに関する民事裁判例」というテーマでの発表内容を元に大幅に加筆したものである。サイバーセキュリティ法制学会の関係者の皆様，そして，西村祥一郎編集長，担当編集者の志田彗様をはじめとする早稲田大学大学院法務研究科 Law&Practice 編集部の皆様に心よりお礼を申し上げたい。

以上