

## 主 文

- 1 原判決を取り消す。
- 2 被控訴人らは、別紙控訴人目録①及び②の各控訴人ら（ただし、同目録①の控訴人番号113及び114の各控訴人らを除く。）に対し、連帯して、それぞれ3300円及びこれらに対する平成26年7月7日から各支払済みまで年5分の割合による金員を支払え。
- 3 控訴人らのその余の請求をいずれも棄却する。
- 4 訴訟費用は、第1、2審を通じて、別紙控訴人目録①及び②の各控訴人ら（ただし、同目録①の控訴人番号113及び114の各控訴人らを除く。）と被控訴人らとの間においては、これを20分し、その19を同各控訴人らの負担とし、その余を被控訴人らの負担とし、別紙控訴人目録①の控訴人番号113及び114の各控訴人らと被控訴人らとの間においては、全部同各控訴人らの負担とする。
- 5 この判決は、第2項に限り、仮に執行することができる。

## 事 実 及 び 理 由

### 第1 控訴の趣旨

- 1 原判決を取り消す。
- 2 被控訴人らは、別紙控訴人目録①及び②記載の控訴人らに対し、連帯して、それぞれ同目録の「請求額」欄記載の金員及びこれに対する平成26年7月7日から支払済みまで年5分の割合による金員を支払え。

### 第2 事案の概要

- 1 本件は、控訴人らが、通信教育事業等を営む被控訴人ベネッセに個人情報を提供していたところ、被控訴人ベネッセからその管理を委託されてい

た被控訴人シンフォームが更に外部業者に再委託をし、そこから更に業務委託を受けた先の会社の従業員において、私物スマートフォンを用いて当該個人情報を不正に取得し、それらを第三者に売却して外部に漏えいさせたことにつき、①被控訴人らには控訴人らの個人情報の管理に係る注意義務違反があった、②被控訴人シンフォームは前記従業員の使用者であり、前記従業員の行為につき使用者責任を負う、③被控訴人ベネッセは被控訴人シンフォームの使用者であり、被控訴人シンフォームの注意義務違反につき使用者責任を負うなどと主張して、被控訴人らに対し、プライバシーの侵害による共同不法行為又は使用者責任等に基づき、連帯して、控訴人らが被った精神的苦痛に対する慰謝料等の損害賠償金（上記漏えいの当時成年であった控訴人らにつき各5万円、未成年であった控訴人らにつき各10万円）及びこれに対する不法行為の後の日である平成26年7月7日から支払済みまで民法所定の年5分の割合による遅延損害金の支払を求める事案である。

2 原審は、前記従業員が控訴人らの個人情報を漏えいした当時、被控訴人シンフォームには、個人情報の不正な漏えい行為を防止するためにスマートフォンを用いた書き出し制御措置を講ずべき注意義務に違反した過失があり、被控訴人ベネッセには、被控訴人シンフォームに対する適切な監督をすべき注意義務に違反した過失があると認められるから、被控訴人らには前記個人情報の漏えいにつき共同不法行為が成立するが、控訴人らには慰謝料請求権を認め得るほどの精神的苦痛が生じたと認めることはできないとして、控訴人らの請求をいずれも棄却した。これに対し、控訴人らが控訴をし、前記第1のと通りの判決を求めた。

3 前提事実、争点及びこれに関する当事者の主張は、以下のとおり原判決を補正し、次項のとおり当審における控訴人らの補充主張を、次々項のと

おり当審における被控訴人らの補充主張を加えるほかは、原判決「事実及び理由」欄の「第3 前提事実」及び「第4 争点及びこれに関する当事者の主張」に記載のとおりであるから、これを引用する。ただし、「原告」を「控訴人」に、「被告ベネッセ」を「被控訴人ベネッセ」，「被告シンフォーム」を「被控訴人シンフォーム」にそれぞれ読み替える（以下同じ。）。

(1) 原判決3頁4行目末尾の次に、改行して以下のとおり加える。

「被控訴人らは、いずれも株式会社ベネッセホールディングス（以下「ベネッセホールディングス」という。）の子会社である。」

(2) 原判決3頁12行目の「委託した」を「委託する旨の業務委託契約を被控訴人シンフォームとの間で締結した。そして、被控訴人シンフォームにおいては、前記システムに関する開発、運用及び保守の業務は、その顧客分析課が主な所管部署とされた。」に改める。

(3) 原判決3頁13行目の「更に」から14行目の末尾までを「外部業者に再委託していた。」に改める。

(4) 原判決6頁2行目末尾の次に、改行して以下のとおり加える。

「(4) 前記顧客情報は、全てサーバコンピュータに記録して保管されており、本件システムの構築作業中の平成25年1月頃から、その一部機能の試行を開始するため、顧客情報が連携システムから本件データベースに入り始めた。当初、本件システムは平成26年4月頃に本格的な運用を開始することが予定されていたが、同時期になってもシステムの不具合が続発していたため、後記の本件漏えいが発覚した同年6月頃にも本格的運用には至っていなかった。（甲63，66，73）」

(5) 原判決6頁3行目の「本件個人情報」の前に「aの業務従事状況及び」を加える。

(6) 原判決 6 頁 4 行目の「被告シンフォーム」から 5 行目の「は、」までを以下のとおり改める。

「被控訴人シンフォームは、本件システムの運用及び保守管理に関して外部業者に再委託をしており、a は、そのような再委託先から更に順次委託を受けて被控訴人シンフォームからみて 3 次委託先となる会社（以下「本件委託先会社」という。）の従業員であった。a は、システムエンジニアとしての経験を有しており、」

(7) 原判決 6 頁 1 2 行目の「6 月頃」の次に「（以下、この頃の時期を指して「本件当時」ということがある。）」を加える。

(8) 原判決 7 頁 4 行目の末尾の次に、改行して以下のとおり加える。

「本件漏えいの事実が発覚したことを受けて、警視庁生活経済課に対する取材に基づき、a が不正に取得した個人情報、教育関連会社等の約 500 社に流出したという報道がされた。（甲 49, 50）」

(9) 原判決 7 頁 5 行目の「乙 1」を「乙 2」に改める。

(10) 原判決 9 頁 8 行目の「業務用」から 1 8 行目の末尾までを以下のとおり改める。

「被控訴人らは、本件当時、情報漏えいを防止するため、業務用パソコンに株式会社日立ソリューションズ（旧商号・日立ソフトウェアエンジニアリング株式会社）の製品であるセキュリティソフトウェア「秘文 Ver. 9.0」（以下「本件セキュリティソフト」という。）を搭載させていた。本件セキュリティソフトは、本件当時、全てのデバイスについて、パソコンからデバイスへのデータの書き出し及びデバイスからパソコンへのデータの読み込みを制御するという接続制御の機能を有していたが、被控訴人シンフォームにおいては、本件セキュリティソフトに MTP による通信について接続を制御する設定を施していなかった。（甲

1, 19の1ないし3, 69ないし71, 乙2)」

(11) 原判決11頁11行目の末尾の次に, 改行して以下のとおり加える。

「(4) 経済産業大臣の勧告について

経済産業大臣は, 平成26年9月26日, 被控訴人ベネッセに対し, 被控訴人ベネッセは, ①その保有する個人情報の利用・管理に責任を持つ部門を設置せず, その安全管理のために必要かつ適切な措置を講ずることを怠っており, 個人情報の保護に関する法律(平成27年法律第65号による改正前のもの。以下「個人情報保護法」という。)20条に違反し, ②顧客情報のシステム開発・運用に関する委託先である被控訴人シンフォームに対して行う定期的な監査において, アラートシステムの対象範囲を監査の対象としていなかったなど, 委託先に対する必要かつ適切な監督を怠っており, 個人情報保護法22条に違反するとして, 個人情報保護法34条1項に基づき, 安全管理措置及び委託先に対する監督の徹底を勧告した。

(甲13の1及び2)

6 aの刑事事件

aは, 平成26年7月17日, 警視庁により不正競争防止法違反の被疑事実に基づき逮捕され, その後, 本件漏えいに係る行為の一部について, 被控訴人ベネッセの営業秘密である顧客情報の不正領得及びその開示行為につき不正競争防止法違反の罪で起訴された。東京地方裁判所立川支部は, 平成28年3月29日, aについて不正競争防止法違反の犯罪の成立を認め, aは顧客情報にアクセスする権限を与えられた者としての地位や専門的知識を悪用し, 極めて大量の顧客情報を領得, 開示した悪質な犯行を行ったものであり, その犯行の結果, 被控訴人ベネッセ及び関連会社の事業活動や経営状態に甚大な悪影響

を与える事態となったなどとして、aを懲役3年6月及び罰金300万円に処するとの有罪判決を宣告した。aはこれを不服として控訴し、控訴審である東京高等裁判所は、平成29年3月21日、aの量刑不当の主張を容れ、aが当該犯行に及んだ背景事情として、被控訴人らにおける顧客情報の管理に不備があるとともに、被害が拡大したことに被控訴人らの対応の不備があり、これらの被害者側の落ち度を考慮すべきであるのに第1審判決の量刑は重きに失するとして、第1審判決を破棄し、aを懲役2年6月及び罰金300万円に処するとの有罪判決（実刑）を宣告した。（甲3，10，19の1及び2，52）」

(12) 原判決13頁23行目の「過失が」から24行目「選択的)」までを削る。

(13) 原判決17頁12行目から13行目にかけての「セキュリティソフトウェア」及び同行目の「同ソフトウェア」をいずれも「本件セキュリティソフト」に改める。

#### 4 当審における控訴人らの補充主張

(1) 本件個人情報の漏えいにつき被控訴人らには予見可能性があったことについて

本件個人情報の漏えいにつき被控訴人らの予見可能性を認めた原審の認定判断は相当であり、以下のとおり、被控訴人らの当審における補充主張についても理由がない。

すなわち、被控訴人らは、本件当時、スマートフォン等の外部機器による情報の不正取得を予見していたからこそ、そのような外部機器に対するセキュリティ対策を行っていたものである。そして、USBメモリ等のUSB機器とパソコンとの間の通信方法として知られるMSC（マストレージクラス〔Mass Storage Class〕の略）

とMTPによる通信方法とが異なる規格であることは事実であるが、一般的なセキュリティソフトウェアにおいては、このような通信方法に着目した設定がされるわけではなく、制御の対象となるデバイスの種別に応じて設定方法が提案されている。このことは、本件当時、被控訴人らに使用されていた本件セキュリティソフト（秘文）においても同様であり、MTPによる通信方法に対応したスマートフォンを含め、MTPデバイスについては、ウィンドウズ・ポータブル・デバイス（以下「WPD」という。）として書き出し制御の対象とする設定が可能であった。

本件当時、被控訴人らの導入していた本件セキュリティソフトを含め、市販されていた多くのセキュリティソフトウェアがWPDに対する制御機能を有しており、WPDが情報漏えいの危険性のある端末であることについては具体的に認識されていたといえる。実際に、被控訴人シンフォームの担当者は、aの刑事事件において、捜査機関に対しWPDについても接続制御機能が有効になっていると考えていた旨述べていたものであり、被控訴人らが、WPDによる情報持ち出しの危険性を認識していたことは明らかである。そして、WPDを利用した情報漏えいが予見できたのであるから、WPDの1機種であるMTP方式のスマートフォンによる情報漏えいについても予見可能性があった。

なお、被控訴人らは、MTPによる通信方法に対応したスマートフォンによる情報漏えいについては結果回避義務がないなどと主張するが、本件セキュリティソフトにおいてWPDについての接続制御機能を有効にする設定をしていなかったのは、クレジットカード情報等を含めた大量の個人情報を取り扱う業者としてリスク管理ができていなかったということにすぎず、結果回避義務がなかったなどということとはできない。

(2) 被控訴人シンフォームの過失責任及び使用者責任が認められること

## ア 過失責任について

被控訴人シンフォームの過失の有無について、原判決が以下の注意義務違反を認めなかった点は不当である。

- (ア) 原判決は、私物スマートフォンの持込み禁止について、執務室（オフィス）につき、持込みを禁止すべき注意義務がないなどとする合理的な理由を説明していない。執務室内には内線電話も設置されており、私物のスマートフォンは業務上使用する必要性がなかったのであるから、持込みを制限すべきであったことは明らかである。
- (イ) また、本件では、アラートシステムが機能していれば情報漏えいを食い止めることができた。すなわち、aは、平成25年7月17日から18日に顧客情報29万1591件を書き出してスマートフォンに保存し、同月18日に株式会社セフティー（以下「セフティー」という。）にこれを売却している。その後、aは、同月29日、同年8月6日に同様の方法で情報を持ち出し、以後も繰り返しているところ、aがセフティーに売却した個人情報の件数1億7897万8933件（甲76）に比較すると、最初の漏えい件数は全体のわずか1.62パーセントであり、その段階でアラートシステムが機能していれば相当割合の漏えいを食い止めることができた。また、アラートシステムが機能していることを掲示していれば、情報の持ち出しをすれば犯人が特定されることで犯行の動機を失わせることもできた。
- (ウ) 被控訴人シンフォームは、執務室を含む施設の主要な入退出口には防犯カメラを設置したものの、一番重要な執務室には監視カメラを設置していなかった。各人の行為が鮮明に記録される監視カメラが設置されていれば、漏えいした情報の出所が判明し、漏えいさせ



たものが特定される可能性が格段に高まるから、犯行を抑止する効力は大きかったのであり、監視カメラに係る注意義務違反を否定した原判決は誤りである。

#### イ 使用者責任について

原判決は、被控訴人シンフォームと a が直接の雇用関係にないことから指揮監督関係にあったことを否定したが、誤りである。

使用者責任における指揮監督関係の有無は、実質的な観点から検討されるべきであるところ、a は、その刑事事件における被告人質問（甲 6 3，6 4）において、①作業ごとに所属していたグループにおいては被控訴人シンフォームの従業員であるリーダーから作業を割り当てられ、打合せへの出席指示を受け、作業スケジュールはリーダーが作成し、WBS と呼ばれる進捗管理表にやるべき作業・担当するメンバーを書き込んでいたこと、② a が在籍する A 社では、雇用契約上、A 社の従業員である T が a を指揮監督する者とされていたものの、a の入社後 1，2 か月が経過した頃には、T と a はそれぞれ別のリーダーの下で作業をするようになり、T も最初は毎日被控訴人シンフォーム多摩事務所に来所していたが、そのうち来所が週 2 日程度に減り、その後は全く来なくなったりしており、例外的に作業の問合せの電話連絡があった程度であったことを具体的に供述している。

また、被控訴人シンフォームの事業開発本部長兼事業開発部長であった b は、a の刑事事件における証人尋問（甲 7 3）において、被控訴人シンフォームの従業員と a のような他の委託先の従業員（以下「パートナー社員」ということがある。）が 1 対 1 でミーティングし、作業工程の確認をし合うことがあることや進捗状況の確認、計画どおりに作業を終わらせるとの要望を出すことがあったこと、パートナー

社員は被控訴人シンフォームに直接作業報告をしていたことなどを認めており、具体的な指示や作業に関する監督があったといえる。

さらに、被控訴人ベネッセと被控訴人シンフォーム間の業務委託基本契約書（甲38）の6条においては、被控訴人ベネッセの事前の書面による承諾のない業務の再委託が禁止されており、aは、本件システム開発に関する事業について、実質的に被控訴人シンフォームの従業員として勤務していたというべきである。

(3) 被控訴人ベネッセの使用者責任が認められること

ア 被控訴人シンフォームの使用者としての責任について

原判決は、被控訴人らの関係が業務委託契約に基づくものであるという形式を重視して、被控訴人ベネッセの使用者責任を否定したが、誤りである。

被控訴人らグループ会社は、従来、被控訴人ベネッセが現在行っている事業を行う会社が親会社として存在し、被控訴人シンフォームはその下でシステムを担当する機能的子会社であった。実質的にみれば、持株会社制に移行する以前は、被控訴人シンフォームは、被控訴人ベネッセのシステム部門がそのまま会社になった機能的子会社という位置付けにあり、被控訴人ベネッセに従属する関係にあったから、実質的には被控訴人ベネッセの指揮監督下にあったといえる。実際に、aを含むパートナー社員は、被控訴人ベネッセの担当者から直接指示を受けていた。また、aは、被控訴人ベネッセとの進捗会議に案件ごとに週1回参加していたし、被控訴人ベネッセの管理職を担う者が被控訴人シンフォームの従業員を兼務して勤務していた。

イ aの使用者としての責任について（当審において追加された主張）

被控訴人ベネッセは、自社のサーバにあるシステムを開発するとい

う業務において、a に対して直接に指揮監督しており、a の使用者にも該当する。このことは、被控訴人らが互いに出向者を在籍させ、上記アで指摘したとおり、被控訴人ベネッセの担当者が、a を含むパートナー社員に対して直接指示をして業務を行わせていたことなどから明らかである。

(4) 違法な権利侵害が認められること

プライバシーの侵害については、正当事由がない限り一般的に違法であって、本件においても違法性について別途検討する必要性はない。

(5) 控訴人らの個人情報がいずれも漏えいしたこと

ア 原判決は、別紙控訴人目録①記載の控訴人番号113及び114の控訴人らの個人情報が漏えいしたとは認められないとしたが、同目録①の控訴人番号115ないし119の住所の一部として「c サマカタ」との情報が漏えいしており、上記番号113及び114の控訴人らの氏のカタカナ表記が漏えいしたものと評価することができるから、同控訴人らも情報漏えいの被害者として認められるべきである。

イ また、原判決は、別紙控訴人目録②記載の控訴人番号12の控訴人の個人情報が漏えいしたとは認められないとしたが、同控訴人は、別件訴訟で情報漏えいが認められた被保護者がお詫びの品として受領した図書券の送付先及び名宛人とされており（甲B12の1及び12の3）、その氏名が被保護者の郵便番号・住所・電話番号と共に情報として保管されていたことが明らかである。被保護者の上記情報が漏えいした以上、保護者である上記控訴人の個人情報も漏えいしたと認められるべきである。

(6) 控訴人らの損害が発生していること

原判決は、本件漏えいについて控訴人らのプライバシーが侵害された

ことを認めながら損害の発生を否定したが、個人情報の現代的価値や要保護性を無視し、その利用可能性や流出による実際の不安を軽視する不当な判断である。

早稲田大学江沢民事件でも、情報漏えいに係る不法行為の成否につき、情報の適切な管理に関する合理的な期待を裏切るものであるかどうかを判断基準とされ、個人情報の秘匿の程度、開示による具体的な不利益の不存在、開示の目的の正当性と必要性などの事情が結論を左右するには足りないとの判示がされている。

被控訴人ベネッセは、本件システムの開発や運用を、被控訴人ベネッセとは契約上も関係性の希薄な者に担当させており、USBケーブルで業務に必要な私物スマートフォンをパソコンに接続することが常態化していることを長期にわたり黙認し、本件セキュリティソフトの設定を誤り、その見直しも行わず放置している間に本件漏えいが行われたものである。aは、セフティーに対して1億7897万8933件の個人情報を売却したことが判明しており、他に2社の名簿業者にも個人情報を売却しているのであって、そこから更に情報が拡散した可能性は否定できず、捜査当局も拡散した先は500社を超えるものと判断している。それらの情報の回収は困難であり、また、拡散した個人情報の悪用の危険性が高いことは明らかであって、控訴人らの損害を否定した原判決は明らかに誤っている。

## 5 当審における被控訴人らの補充主張

### (1) 本件漏えいに関する被控訴人らの予見可能性について

本件漏えいに関して、被控訴人らの予見可能性を肯定するためには、従来の一般的なスマートフォンのパソコンへの接続方式（通信規格）はMSCであって、本件セキュリティソフトの書き出し制御措置はUSB

による接続方式（通信規格）がM S Cであれば機能するが，M T Pであれば機能しないものであったこと，本件当時までに販売されるようになった一部のスマートフォンはM T Pによる通信方法に対応していたことを具体的に認識していたことが必要である。

しかるところ，被控訴人シンフォームが本件セキュリティソフトを導入し書き出し制御措置を設定したのは平成23年夏であったところ，その時点では，M T Pに初めて標準対応したスマートフォン用O SであるA n d r o i d 4 . 0を搭載したスマートフォンも発売されていなかったのものであって，被控訴人シンフォームとしては，書き出し制御措置を講じることによってスマートフォン一般について書き出し制御できるものと考えていた。M T PによりM S Cデバイス制御に抜け道が生ずるといふ危険性については，本件当時，情報セキュリティの専門家においても認識されていなかったのもであり，被控訴人シンフォームは，本件セキュリティソフトの単なるユーザーにすぎず，セキュリティソフト会社から一部のスマートフォンには対応できない状態になっているなどの注意喚起を受けることもなかったのもであって，そのようなセキュリティソフトウェアの穴に気付く契機はなかった。本件当時までにM T Pによる通信方法に対応したスマートフォンへの情報書き出しの危険性について具体的に指摘した行政機関その他の団体のガイドライン等はなかったのもであり，被控訴人らの予見可能性の有無については，例えば経済産業分野ガイドラインにおいて「しなければならない」とされている事項を充足していたかなどの観点から検討すべきである。M T Pは，もともとデジタルカメラやデジタルビデオカメラ，携帯音楽プレーヤー，ボイスレコーダー等をウィンドウズパソコンに簡便に接続するために用いられていた技術仕様であり，本件当時，M T Pによる通信を行う機器としては，ス

スマートフォンは念頭におかれていなかった。前記機器は情報漏えいのリスクとしてとらえられていなかったことから、情報漏えいの対策としてMTPによる通信を制御するという発想も実践もなかったのである。

また、原判決は、①書き出し制御措置は実効性があり、②業務従事者に対して必要以上に制約が生じない方法であることから、結果回避義務を認めているが、これは過失をレトロスペクティブ（事後的・後方視的）に捉え、こうすれば結果が生じなかったのだからこうすれば良かったとして、結果責任を認めるもので誤りである。過失は、行為当時の一般的水準に照らして、プロスペクティブ（事前的・前方視的）なものとして確定されなければならない。

## (2) 被控訴人シンフォームの過失責任及び使用者責任について

ア 原判決が、被控訴人シンフォームの書き出し制御措置に関する注意義務違反を認めた点は、不当である。本件セキュリティソフトは、そもそもMTPにより通信をするデバイスに対する書き出し制御機能を有しておらず、MTPによる通信につき読み取りも書き出しも不可とする接続制御機能しか有していなかった。控訴人らの主張は、あらゆる機器へのパソコンへの接続を一律に禁止すべきであるかのようであるが、パソコンの使用によって得られる利便性を合理的根拠なく放棄すべきというに等しい暴論である。

### イ 使用者責任について

a の刑事事件における供述内容は、被控訴人シンフォームにおける仕事の割り振りや日常的な業務指示等の具体的場面について述べることなく、抽象的に、被控訴人シンフォームの従業員であるリーダーが直接、委託先要員に仕事を割り振り、日常の業務指示をしていたという結論のみを述べるものにすぎない。

a は、刑事事件において、被控訴人シンフォームから直接指揮命令を受けていたため、被控訴人シンフォーム以下の契約関係は偽装請負であり公序良俗違反により無効であるから、a が営業秘密を管理する任務を負っておらず無罪であるとの主張をしていたのであり、虚偽供述への強い動機があるとみななければならない。

(3) 被控訴人ベネッセの過失責任及び使用者責任について

ア 被控訴人ベネッセには、被控訴人シンフォームに対してMTPによる通信方法に対応したスマートフォンへの書き出し制御措置をとるよう指示すべき義務はなかった。委託業者と受託業者は、法人として異なるのであり、受託業者に業務遂行に当たり過失があったとしても、特段の事情がなければ委託業者に過失があることにはならない。被控訴人ベネッセが、被控訴人シンフォームに対し、適切に報告を求めていたとしても、被控訴人ベネッセが書き出し制御措置の不十分な点に気付く可能性はなかったから、監督義務違反は認められない。

イ システム開発やシステム保守運用その他委託元に常駐する形態の業務委託（かかる形態をとらざるを得ないのは、業務の性質上、必然的である。）について、問題が発生した場合にはすべからず委託元が指揮監督をしていたなどと判断するのは不当である。被控訴人ベネッセと被控訴人シンフォームとの関係は業務委託契約という対等な取引関係であり、被控訴人ベネッセは、被控訴人シンフォームの使用者とはいえないし、a の使用者とされる具体的根拠は存在しない。

(4) 違法な権利侵害の有無について

プライバシー侵害の事案にあつては、法益侵害の有無とは別に違法性の有無の検討が必要である。違法性の有無の判断は、被侵害利益の性質と侵害行為の態様を相関関係的に考量してされるものであるが、被侵害

利益の要保護性が弱く、また侵害行為の態様について社会的相当性の逸脱の程度が低いほど、違法性は否定されやすくなる。本件個人情報の内容や性質は、本来社会生活を送るうえでは当然明らかにされるべき個人識別などのための単純な情報にとどまり、情報の利用によって初めて個人の社会関係、取引関係、法律関係等の様々な関係が円滑に行われ得るものであって、秘匿されるべき性質のものとはいえず、被侵害利益の要保護性は低い。被控訴人らの侵害行為の態様として悪質性がほぼ存在しないことや事後的に速やかな公表、補償、原因究明及び再発防止策の検討と実施を含む対応措置をとったことなどを考慮すれば、一般人の感受性を基準として、被控訴人らの行為が、社会的に容認されないものとして違法であるとみる余地はない。

(5) 控訴人らの個人情報の漏えいの有無について

ア 別紙控訴人目録①記載の控訴人番号113, 114の控訴人らについて、「c」が上記控訴人らに関する情報であると特定することは困難である。そもそも、上記番号115ないし118の控訴人らの住所の内容として「c」との情報が含まれてはいなかったし、同119の控訴人の住所の内容に「cサマカタ」が含まれていたとしても、その地域にcという姓を有する個人が居住していることは住宅地図によって広く公開された情報にすぎない。

イ 別紙控訴人目録②記載の控訴人番号12の控訴人について、控訴人ら指摘の送付書（甲B12の1及び12の3）に同控訴人の氏名が記載されていたとしても、同送付書には本件漏えいが判明した後に登録された情報が宛名として記載された可能性があり、控訴人らの主張には理由がない。

(6) 控訴人らの損害の発生の有無について



控訴人らが本件漏えいによる損害として主張するのは、抽象的な不安や不快感にすぎず、これによって平穏な生活を送る利益が害されるとは一般に考えられない軽微なものである。本件漏えいに係る行為の前後で控訴人らのおかれた具体的な立場や状況には変化がなく、損害は発生していない。秘匿性の高くない個人情報の流出に対して、具体的損害がないにもかかわらず損害の発生を認めて安易に損害賠償を認めることは、不法行為制度の目的からも正当化されるものではない。

本件漏えいによって、何らかの本件個人情報を取得した漏えい先が500件を超えるという事実については客観的根拠がなく、控訴人らの個人情報が直接の売却先を超えて拡散した事実は何ら認められない。

### 第3 当裁判所の判断

当裁判所は、本件漏えいについて、被控訴人らには控訴人らの個人情報の管理に係る注意義務違反があり、かつ、個人情報が漏えいした控訴人ら1人につき各3300円の損害賠償請求（3000円の慰謝料及び300円の弁護士費用相当額）を認めるのが相当であると判断する。その理由は、以下のとおりである。

1 認定事実（前記前提事実に加え、掲記の証拠（ただし、いずれも以下の認定に反する部分は除く。）及び弁論の全趣旨によれば、以下の事実が認められる。

(1) aの勤務状況と本件漏えい行為について

ア aは、システムエンジニアであり、本件システム構築等の業務について被控訴人シンフォームから再委託を受けた会社から更に再々委託を受けた会社の従業員であった。aは、平成24年4月から、被控訴人シンフォーム多摩事務所の執務室において稼働を開始し、顧客分析課の開発チームのグループに属して作業に従事していた。

被控訴人シンフォームでは、事業開発本部の下に事業開発部がおかれ、事業開発部の中に顧客分析課がおかれており、顧客分析課が本件システム構築等の業務を所管していた。顧客分析課には、平成26年6月当時、39名が所属しており、そのうち被控訴人シンフォームの従業員は11名であり、その余の28名は、aを含む他の委託先の従業員であり、パートナーないしパートナー社員などと呼ばれていた。

顧客分析課の中には複数のチームがあり、各チームの中には個別案件を効率的に進めるために少人数で構成された複数のグループがあり、各グループには、被控訴人シンフォームの社員であるリーダーが置かれていた。そして、各グループでは少なくとも毎週1回は進捗会議が開かれ、同会議にはグループメンバー全員が参加して作業状況や作業予定等についての打合せがされていた。

(以上につき、甲19の1ないし3，甲63，64，66，73，88の1)

イ aは、被控訴人シンフォームの業務に従事する前に、被控訴人シンフォームから、業務上知り得た個人情報及び機密情報を開示・漏えいしないことを誓約する内容の「個人情報の取扱いに関する同意書」を提出し、また、被控訴人シンフォームが行う情報セキュリティ研修及びその内容を踏まえたテストを受け、その後も年1回実施される情報セキュリティ研修を受けていた。(前記前提事実1(2)，甲2，19の1ないし3，63，88の1)

ウ aは、平成25年6月頃、経済的に困窮した状況であったことから、被控訴人ベネッセの顧客情報を名簿業者に売却して金員を得ることを思いついたが、業務上用いていたパソコンには、USBメモリ等の外部記録媒体を接続してもパソコンに認識されず、顧客情報を持ち出せ

ない措置が講じられていたことから、そのようなことはできないと諦めていた。ところが、平成25年7月頃、本件スマートフォンを充電するために市販のUSBケーブルを用いて業務用パソコンのUSBポートに接続し充電していたところ、パソコンにスマートフォンが外部記録媒体として認識され、パソコンの画面にスマートフォン内のフォルダが表示されたことから、試しにパソコンからファイルを転送してみたところ、スマートフォンに保存することができた。(甲63, 88の1及び2)

エ aは、平成25年7月頃から平成26年6月頃までの間、被控訴人シンフォーム多摩事務所において、被控訴人ベネッセの顧客情報を業務用パソコンから本件スマートフォンに転送し、その内蔵メモリに保存する等の方法により個人情報を不正に取得した。

本件スマートフォンは、平成24年秋冬期に発売された「au HTC社製 HTL21」という機種であり、OSはAndroid 4.1であった。前記スマートフォンには、データ通信方法としてMTPが初期設定されており、前記転送はMTPを用いて行われたものであった。

(以上につき、前記前提事実3(2)、甲11の1及び2、甲12の1及び2、63、64、88の1及び2)

## (2) MSCとMTPについて

ア MSCとMTPは、いずれもパソコンとこれに接続された各種デバイスとの間の情報通信方式(ファイル転送プロトコル)である。

MSCは、パソコンとUSBメモリやメモリカード等のデバイスである外部記憶装置・媒体との間の情報通信方式として用いられているものであり、MTPは、WindowsをOSとするパソコンと携帯

機器との間で音楽・動画等のマルチメディア・データを簡便に共有・連携できるようにするためにマイクロソフト社が開発した規格であり、デジタルカメラの画像転送プロトコル（PTP）をベースに、音楽・動画ファイルなどの転送を可能にした技術仕様である。

MSCでもMTPでも、パソコンにスマートフォンなどのデバイスをUSBケーブルで接続してデータの転送をすることが可能である点で違いはないが、ファイルシステムの管理等について、MSCではパソコン側のOSで行われ、接続されたデバイスはUSBに接続された外部記憶装置（USBメモリや外付けHDDなど）と同じく認識されるのに対し、MTPではデバイス側で行われ、接続されたデバイスはWPDなどとして認識される。

（以上につき、甲15、16、98の1ないし4、乙33、101）

イ スマートフォンの主なOSには「iOS」及び「Android」がある。MTPによる通信方法は、前記アの開発経緯から、従来は音楽・映像プレーヤーやデジタルカメラ等に利用されており、スマートフォンについては、「iOS」はMTPによる通信方法に対応していないが、「Android」については、平成23年10月18日に発売されたAndroid 4.0以降のバージョンがMTPによる通信方法に対応するようになった。

そして、株式会社NTTドコモ、KDDI株式会社及びソフトバンクグループ株式会社が平成24年夏に発売したスマートフォンには、OSをAndroid 4.0とするものが多数あり、また、電気通信事業者各社は、Android 4.0より前のバージョンのスマートフォンについて、その頃以降、OSのバージョンアップを提供した。なお、同年8月頃に発売されたサムスン製の「GALAXY S II

W I M A X I S 1 1 S C」の取扱説明書には、メディア転送モード（M T P）でU S Bケーブルを用いてパソコンと当該スマートフォンを接続すると、パソコンに当該スマートフォンがポータブルデバイスとして認識され、当該スマートフォンとパソコンとの間でデータのやりとりができることが明記されている。

（以上につき、甲16, 51の1ないし3, 105の1ないし6, 115, 乙33）

ウ M T Pによる通信方法に対応したスマートフォンの発売及びその普及等について、本件当時までにメディア等に取り上げられたものとして以下のような記事の存在を指摘することができる。

(ア) インターネット上の「モバイルトレンド」という連載において、平成23年4月27日に掲載された「スマートフォンのパソコン接続は大容量デバイスからM T Pへ（第164回）」と題する記事の中で、テクニカルライターの塩田紳二は、最近登場したA n d r o i dスマートフォンやタブレットでは、パソコンとの接続にM T Pを使うものが増えてきたことを述べて、従来用いられてきたM S Cによる通信方法との違いについて説明をし、M T Pを用いるメリットやデメリットに言及した上、今後はM S CよりM T Pの方が便利な通信方法としてスマートフォンやタブレットでは、M T Pを採用するものが増えていきそうであると記載をした。（甲15）

(イ) 「日経P C 2 1」という雑誌において、平成24年12月24日発売の2013年2月号版に掲載された「スマホはパソコンと連携して使うのが正しい！ 3つの方法を完全習得」と題する記事の中で、スマートフォンとパソコンとの間でファイルをやりとりする3つの方法のうち、1つがU S Bケーブルを用いて接続する方法とし

てMTP（メディア転送プロトコル）とMSC（大容量ストレージ）の2種類を指摘することができる。両方の方式が使えるスマートフォンならより簡単なMTPを使うとよいこと、その方法によるとスマートフォンとパソコンをケーブル接続するだけでスマートフォン内の記憶装置がリムーバブルディスクとして表示されることなどが記載されていた。前記記事は、平成25年6月5日に「日経トレンドネット」のウェブサイト上にも掲載された。（甲116）

(3) 被控訴人シンフォームによる安全管理措置及び本件セキュリティソフトの設定について

ア 被控訴人シンフォームでは、業務での私物パソコンの使用を禁じ、全従業員個人に対して、所定の設定がされた業務用パソコンを貸与した上、IDを付与し、90日に一度の頻度で変更を要するパスワードを設定させて利用させていた。業務用パソコンは、業務上の必要がない限り社外への持ち出しは禁止され、通常は施錠付きチェーンで各人のデスクに固定されていた。その他、本件当時、被控訴人シンフォームが情報管理のために採用していた安全管理措置については、前記前提事実4記載のとおりである。（甲19の1ないし3、乙2）

イ 被控訴人らは、従業員に貸与していた業務用パソコンに本件セキュリティソフトを搭載しており、平成23年7月に前記業務用パソコンのOSをWindows 7にバージョンアップした際、本件セキュリティソフトも当時の最新版である「秘文Ver. 9.0」にバージョンアップした。

本件セキュリティソフトは、前記のとおりバージョンアップされた際に、「リムーバブル、CD/DVD、外付けHDD」の他、終端機器としてイメージングデバイス、WPD、ウィンドウズモバイル、ブ

ラックベリ等デバイス、通信機器として無線LAN、モデム、赤外線等を接続制御することが可能となっていた。前記デバイスのうち「リムーバブル、CD/DVD、外付けHDD」については、データの書き出し制御のみを設定することが可能であり、リムーバブルメディアについては、組織で管理していないUSBメモリの個体識別制御が可能であった。また、読み書きを個別に許可されたUSBメモリについては、書き出されたデータは暗号化された。WPDを含む前記以外のデバイスについては、書き出し制御のみの設定をすることはできず、接続制御のみが可能であった。そして、前記デバイスの全てを制御した場合、パソコンからデータの書き出しをすることは不可能な状態にすることができた。

(以上につき、甲69ないし71)

ウ 本件セキュリティソフトの販売代理店は、本件セキュリティソフトのバージョンアップの際、その設定作業を行ったところ、被控訴人シンフォームとしては、特定のUSBメモリ以外の全ての外部記録媒体への書き出しを制御するとの方針をとっていたが、実際には、本件セキュリティソフトのバージョンアップの際の設定内容は、「リムーバブル、CD/DVD、外付けHDD」だけが書き出し制御の対象とされ、WPDを含む他のデバイスについては接続制御機能を有効とする設定が行われなかった。そして、前記販売代理店は、平成23年8月、被控訴人シンフォームに対してパラメーターシートを納品し、そこには、本件セキュリティソフトの設定内容として、「デバイス制御設定」欄の「①デバイス使用可否制御を有効にする、②デバイス個体識別制御を有効にする、③個体識別ログの出力を有効にする」の3つの項目のチェック欄にチェックがされておらず、設定されていないことが明

示されていた。

本件セキュリティソフトは、ユーザーにおいても作業手順を踏むことによって、制御可能な個々のデバイスについて、制御の有無の設定内容を自由に変更できるものであったが、aによる本件漏えいが発覚した後の平成26年7月に、後記エのとおり本件セキュリティソフトはWPDにつき接続制御機能を有効とする設定に変更されたが、それまでの約3年間は、本件セキュリティソフトの設定内容の変更はされなかった。

(以上につき、甲12の1及び2、66、69ないし71)

エ 被控訴人シンフォームは、本件漏えいが発覚した後の平成26年7月22日に本件セキュリティソフトのバージョンアップを行い、また、設定の見直しをして、「リムーバブル、CD/DVD、外付けHDD」の書き出し制御機能の他に、イメージングデバイス、WPD、ウィンドウズモバイル、ブラックベリー、無線LAN、モデム、赤外線等のデバイスの接続制御機能を有効にした。(甲19の1ないし3)

オ 商用デバイス制御ソフトの製品がMTP使用制限機能に対応した時期は、遅くとも以下のとおりであり、下記各製品の国内市場におけるシェアは、平成26年6月時点で合計すると43.5パーセントであったことが認められる。(甲16、69、96の1ないし5、97、101の1及び2、103の1、乙36、113の1)

企業名	製品名	対応時期
日本電気株式会社	InfoCage	平成19年7月
株式会社日立ソリューションズ	秘文 AE Information Fortress	平成21年6月
エムオーテックス株式会社	LanScope Cat	平成25年10



		月
日本ファインアート株式会社	TotalSecurityFort	平成23年8月
ハミングヘッズ株式会社	Evolution/SV	平成23年12月
株式会社インテリジェントウェイブ	CWAT	平成24年7月
富士通株式会社	Systemwalker Desk top Keeper	平成25年8月
C&Cアソシエイツ	発見伝	平成25年8月
クオリティソフト株式会社	QND Advance	平成25年9月
米国 DeviceLock 社	DeviceLock	平成26年2月

## 2 本件漏えいに関する被控訴人らの予見可能性について

- (1) 本件漏えいに係る行為は、aにおいて、貸与されていた業務用パソコンから本件データベースにアクセスし、本件データベース内に保管されていた本件個人情報を抽出して業務用パソコンに保存した上、USBケーブルを用いて、MTPによる通信方法に対応する本件スマートフォンに転送したというものである（前記前提事実3(2)）。

このようなMTPによる通信方法を用いたデータの転送については、もともとMTPが、WindowsをOSとするパソコンと携帯機器との間で音楽・動画等のマルチメディア・データを簡便に共有・連携できるようにするために開発された規格であり、パソコンとUSBメモリやメモリカード等のデバイスである外部記憶装置・媒体との間の情報通信方式として、従来のスマートフォンで多く使用されていたMSCとは異なる規格であったことに照らすと、被控訴人らの本件漏えいに関する予見可能性の有無を検討するに当たっては、MSCに限らず、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の認識可能性があったといえるかどうかを検討すべきものと解される。

- (2) そこで検討するに、本件当時も、スマートフォンをUSBケーブルでパソコンと接続しデータのやりとりをすることが可能であることは一般的に知られており、本件漏えいの以前から、例えば経済産業分野ガイドライン（平成21年10月9日の告示）が、個人情報保護法の基本理念を踏まえ、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しい事項の例として、「個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定（例えば、個人データを入力できる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにする。）」などと記載されており、外部記録媒体をパソコン等に接続する方法による情報漏えいのリスクが指摘されていたこと（甲7，9，乙11）が認められる。

そして、前記認定事実のとおり、MSCとMTPは、いずれもパソコンとこれに接続された各種デバイスとの間の情報通信方式（ファイル転送プロトコル）であって、本件漏えいに係るaの行為も、本件スマートフォンを充電するために市販のUSBケーブルを用いて業務用パソコンのUSBポートに接続し充電していたところ、上記パソコンにスマートフォンが外部記録媒体として認識されたため、試しに上記パソコンからファイルを転送してみたところ、スマートフォンに保存することができたというものであって、格別専門的な知識や道具等を用いてデータの転送をしたわけではない。本件当時には、既にMTPによる通信方法に対応したスマートフォンが多数発売され、又はMTPによる通信方法に対応するようにバージョンアップすることも可能な状況であったこと（前

記認定事実(2))，情報管理に関する社会一般の認識という観点からみても，株式会社日立ソリューションズを含めた相当数の大手業者が，本件漏えいが発覚する以前からMTP使用制限機能に対応した商用デバイス制御ソフトの製品を販売するようになっており（前記認定事実(3)），被控訴人シンフォームも，平成23年7月に本件セキュリティソフトをバージョンアップした際には，特定のUSBメモリ以外の外部記録媒体についても書き出しを禁止するという方針をとっていたものであること（前記認定事実(3)），加えて，スマートフォンは，従来の通話機能のみを基本的な機能とする携帯電話とは異なり，小型のパソコンともいえる多彩な機能を有する機器であって，年々バージョンアップによる機能の高度化が進むデバイスであることを併せ考慮すれば，被控訴人らは，本件当時，MSCに限らず，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，すなわち，本件漏えいに関する被控訴人らの予見可能性はあったというべきである。

- (3) これに対し，被控訴人らは，①実際には，本件漏えいの時点においてMTPによる通信方法に対応したスマートフォンの国内シェアは小さかったし，商用デバイス制御ソフトの製品のうちMTP使用制限機能に対応したものもなかった，②本件漏えいによって初めて，スマートフォンを利用した個人情報の不正取得の危険性が認識されるようになったのであり，それ以前は専門家にとってもMTPによる通信方法を利用したデータの転送により，MSCデバイス制御に抜け道が生ずるという危険性について一般的な認識とはなっていなかった，③本件当時までにMTPによる通信方法に対応したスマートフォンへの情報書き出しの危険性について具体的に指摘した行政機関その他の団体のガイドライン等はなか

ったなどと主張する。

- (4) 前記①について、被控訴人らは、本件当時、MTPによる通信方法に対応したスマートフォンの国内シェアが少なかったことに関し、株式会社インターネットプライバシー研究所が作成した「携帯電話端末におけるMTP普及率についての調査報告」（乙35）を提出し、そこには、スマートフォンと従来の携帯電話を併せた台数に対するスマートフォンの割合は、平成24年3月末で22%、平成25年3月末で36%、平成26年3月末で48%であり、MTPによる通信方法に対応したスマートフォン（「Android 4.0」以降のOSを搭載したもの）のスマートフォン全体における割合は、平成24年6月時点で0.69%、平成25年6月時点で19.88%、平成26年6月時点で21.41%であったこと、また、平成26年のスマートフォンの出荷台数が2770万台であったことが記載されている。これによれば、平成26年6月頃のMTPによる通信方法に対応したスマートフォンの出荷台数は、593万台余りということになる。

しかし、仮に前記の報告を前提にしたとしても、MTPによる通信方法に対応したスマートフォンの国内シェアについては、平成23年10月18日に発売されたAndroid 4.0以降のバージョンがMTPによる通信方法に対応するようになり、株式会社NTTドコモ、KDDI株式会社及びソフトバンクグループ等の大手業者が平成24年夏に発売したスマートフォンには、OSをAndroid 4.0とするものが多数出てきていたことや、OSのバージョンアップも提供されていた事実（前記認定事実(2)）からすると、遅くとも本件当時までには、国内において、MTPによる通信に対応したスマートフォンの普及率が高まり、相当多数の台数が販売されるようになっていく状況にあったということ

ができるのであるから、前記の報告が、MTPによる通信方法に対応したスマートフォンによるデータの転送について、被控訴人らの予見可能性を否定するものとはいえない。

また、前記①のうち商用デバイス制御ソフトの製品のうちMTP使用制限機能に対応したものもなかったという点について、被控訴人らは、株式会社インターネットプライバシー研究所が作成した「端末管理・セキュリティ製品におけるMSC・MTP制御機能についての調査報告」

(乙36)を提出し、そこには、平成26年6月当時販売されていた主要な端末管理・セキュリティ製品について、実用的なMTP制御機能は、国内市場シェアが高い製品については全く搭載されておらず、実用的なMTP制御機能を搭載していたと認められる製品は、国内市場シェアが微少な1製品にとどまり、かつ初期設定ではMTP制御機能は無効とされていた旨の記載がある。しかし、前記報告においては、「実用的」の意味を「少なくとも読み取り専用の設定（リムーバブルメディアからパソコンにデータを転送することは可能であるが、パソコンからリムーバブルメディアにデータを転送することは不可能とする設定）ができる場合」と定義し、「実用的」でない製品についてはMTP制御機能を搭載していないものとして扱っているところ、情報セキュリティの観点からパソコンに保存されている情報を管理したり、当該パソコンを通じて情報を管理したりする場面において、リムーバブルメディアからパソコンにデータを転送すべき場合を想定する必要性に乏しく（甲15によれば、もともとMTPの規格は、音楽ファイル等を転送するために開発された規格であるとされている。）、双方向の転送のいずれもが制限されることから情報セキュリティ上「実用的」でないとするのは不合理である。したがって、同報告は、その前提を欠くものといわざるを得ず、採用す

ることはできない。

- (5) また、前記②について、被控訴人らは、特定非営利活動法人日本ネットワークセキュリティ協会dで理事及び事務局長を務めるとともに一般社団法人日本スマートフォンセキュリティ協会dで理事を務める d の意見書（乙 3 3）を提出し、そこには、本件漏えいによって初めて、パソコンのリムーバブルメディアとしてスマートフォンを含む携帯電話が使用される危険性があることが認識され、セキュリティ業界がその対策をとるようになったのであり、大手セキュリティベンダーでさえ予見できていなかったものを、ユーザーである被控訴人シンフォームが予見することは不可能であったという趣旨の記載がある。さらに、株式会社インターネットプライバシー研究所は、被控訴人らから依頼を受けて複数の意見書等を作成し、平成 2 9 年 1 月 2 3 日付け意見書（乙 2 5）及び平成 3 0 年 9 月 2 0 日付け意見書（乙 9 7）の中では、本件当時、MTP による通信方法に対応したスマートフォンによる情報漏えいのリスクは、情報セキュリティ専門家の間でもほとんど認識されていなかったと指摘し、平成 3 0 年 9 月 2 0 日付け意見書の中では、一般の企業等の業務において、デジタルカメラやボイスレコーダー等の画像・動画・音声の情報を MTP による通信方法によりパソコンに取り込むことは日常的に行われており、MTP による通信について読み取りを制御すれば、業務上大きな支障が生ずることを指摘している。そのほか、被控訴人らは、本件漏えいの方法による情報漏えいの危険性を予見できなかったことについて情報セキュリティの専門家等の記事（乙 3 7, 3 8）を提出し、また、当審において新たに工学院大学名誉教授 e が作成した平成 3 0 年 1 月 1 5 日付け意見書（乙 9 2）を提出し、そこには、本件当時、MTP による通信方法を利用した情報漏えいの危険性は知られていなかったとの認

識についての記載がある。

しかし、本件当時までに、MTPによる通信方法に対応したスマートフォンを利用したデータの転送が可能であることについてメディア等に取り上げられたものがなかったわけではなく（前記認定事実(2)）、前記のとおり、スマートフォンは小型のパソコンともいえる多彩な機能を有する機器であって年々バージョンアップによる機能の高度化が進むデバイスであり、実際にMTPによる通信方法に対応したスマートフォンの普及率が高まるとともに、MTP使用制限機能に対応した商用デバイス制御ソフトの製品が、平成19年以降、平成25年8月頃までには多数の販売業者によって販売されている状況下にあったこと、被控訴人らも特定のUSBメモリ以外の全ての外部記録媒体への書き出しを制御するとの方針の下で本件セキュリティソフトを搭載していたことからすれば、MTPによる通信方法に対応したスマートフォンへの情報書き出しの危険性について具体的に指摘した行政機関等のガイドラインがなかったとしても、被控訴人らにおいて、新たに登場したMTPによる通信方法に対応したスマートフォンに対する情報漏えいの危険性があり、その対策の必要性があることについて認識し得たというべきである。

以上によれば、被控訴人らが主張する前記②の点及び前記③の点について考慮したとしても、本件漏えいに関する被控訴人らの予見可能性についての前記認定判断を覆すものとはいえない。

### 3 被控訴人シンフォームの過失責任について

#### (1) 執務室への私物スマートフォンの持込み禁止について

本件において、aが執務を行う部屋に、私物のスマートフォンを持ち込むことを禁止する措置をとっていれば、本件漏えいを回避できたということが出来るが、個人情報等の情報を扱う以外にも通常業務を行う

ような執務環境において、私物のスマートフォンの持込みを一切禁止するというのは、当該執務環境において従事する者にとって、非常に大きな制約となることは明らかであり、加えて、後記(3)に説示するとおり、同様の効果を上げられる他の代替手段があり得ることに照らすと、被控訴人シンフォームにおいて、本件当時、執務室内に私物のスマートフォンの持込み禁止措置を講ずべき注意義務があったということはできない。

控訴人らは、①安全対策基準には、「搬出入物」について、「情報システム等の運用に関連する各室の搬出入物は、必要な物に限定すること。」との記載があり、②内部不正防止ガイドラインには、個人のノートパソコンやスマートデバイス等のモバイル機器及び携帯可能なUSBメモリ等の外部記録媒体の業務利用及び持込みを制限しなければならない旨の指摘があり、③データセキュリティガイドブックには、共有区画として、オフィスとサーバー室に区別され、サーバー室については、脅威として情報の不正持ち出しの指摘とともに、管理策として記録媒体の持込み禁止ルールの記載があることに照らすと、被控訴人シンフォームには、本件漏えい当時、執務室内に私物のスマートフォンを持ち込むことを禁止すべき注意義務があったと主張するので、以下検討する。

#### ア 安全対策基準について

確かに、安全対策基準（甲6）には、「搬出入物」について、「情報システム等の運用に関連する各室の搬出入物は、必要な物に限定すること。」と記載されている。

しかし、当該記載から、私物スマートフォンを上記の搬出入物の対象としているかどうか明らかとはいえない。かえって、安全対策基準が改正されたのは、平成9年が最後であるところ、同年当時、スマートフォンが市場で流通していたことを認めるに足りる証拠はないから、



少なくとも、安全対策基準が具体的にスマートフォンを念頭に置いて策定されたとは考え難い。

そうすると、安全対策基準から、被控訴人シンフォームについて当然に私物スマートフォンの執務室内への持込みを禁止すべき注意義務があるとは認められない。

#### イ 内部不正防止ガイドラインについて

確かに、内部不正防止ガイドライン（甲9）においては、個人のノートパソコンやスマートデバイス等のモバイル機器及び携帯可能なUSBメモリ等の外部記録媒体の業務利用及び持込みを制限しなければならないとの指摘があるが、他方で、対策のポイントとして、持込み制限では、その場所で扱う重要情報の重要度及び情報システムの設置場所等を考慮する必要がある旨の記載があり、また、「重要情報の格納サーバやアクセス管理サーバ等が設置されているサーバールームでは、個人所有のノートPCやタブレット端末、スマートフォン等のモバイル機器の持ち込み、利用を厳しく制限します。」とも記載されていることに照らすと、内部不正防止ガイドラインは、いかなる業務が行われている部屋であっても同様の持込み制限を講じる必要があるという趣旨を示すものではなく、その扱う情報の重要度や情報システムの設置場所に応じた対策をとるべきとの趣旨を示すものであると解すべきである。そうすると、重要な情報が直接格納されているサーバの所在する場所では、外部記録媒体をより直接的にサーバ等の機器に接続することが可能であり、当該情報により直接的にアクセスすることが可能となることから、そのような可能性を高い確率で制限できる措置をとる必要があると考えられるが、通常の執務室のように、そのような直接的なアクセスではなく、別のサーバや機器を経由して、当該情報

に接することができるにすぎない場合には、内部不正防止ガイドラインは、必ずしもそのような厳しい制限をすることまで要求していないと解するのが相当である。

そうすると、内部不正防止ガイドラインから、当然に私物のスマートフォンの執務室内への持込みを禁止すべき注意義務があるとは認められない。

#### ウ データセンターセキュリティガイドブック

確かに、データセンターセキュリティガイドブック（甲20）では、共有区画として、オフィスとサーバー室に区別され、サーバー室については、脅威として情報の不正持ち出しの指摘があり、管理策として記録媒体の持込み禁止ルールの記載があるが、他方で、オフィスについて、その脅威として不正侵入の指摘があるのみで、管理策として画像監視システムと入退管理システムの記載（ICカード・生体認証）があるにとどまることに照らすと、データセンターセキュリティガイドブックの記載を根拠に、当然にスマートフォンの執務室内への持込み禁止措置をとるべき注意義務があるとは認められない。

したがって、この点に関する控訴人らの主張は理由がない。

#### (2) 業務用パソコンに対するUSB接続禁止措置について

確かに、物理的にパソコンのUSBポートを塞ぐことで、業務用パソコンを使用する者が自由にパソコンにUSB接続できないようにすれば、本件漏えいの方法による情報漏えいを防ぐことができたといえる。

しかし、パソコンのUSBポートは、外部記録媒体の接続以外にも、マウスを使用する際に用いるなど、業務上必要な装置を接続することが想定されている。控訴人らは、マウスについて、USBポートによる接

続以外の方法での接続が可能であると主張するが、どのようなマウスであっても別の方法での接続が可能であると認めるに足りる証拠はなく、また、仮にその点をおくとしても、後記(3)で説示するとおり、同様の効果を上げられる他の代替手段があり得ることに照らすと、USBポートを使用できなくするという措置は、スマートフォンの持込み禁止措置ほどではないにしても、業務に従事する者に対する制約として過度なものであるといわざるを得ない。

したがって、被控訴人シンフォームにおいて、本件漏えい当時、業務用パソコンのUSB接続の禁止措置を講ずべき注意義務があったということとはできない。

この点について、控訴人らは、①経済産業分野ガイドラインには、個人データを入力できる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにする旨の記載があること、②内部不正防止ガイドラインでは、個人の情報機器及び記録媒体を持ち込まれた場合の情報持ち出しのリスクや、外部記録媒体の業務利用を制限することを対策のポイントとして掲げていること、また、③マネジメントシステム実施ガイドラインでは、経済産業分野ガイドラインと同様の記載があることに照らすと、被控訴人シンフォームには、本件漏えい当時、業務用パソコンのUSB接続の禁止措置を講ずべき注意義務があったと主張するので、以下検討する。

#### ア 経済産業分野ガイドラインについて

確かに、経済産業分野ガイドライン（甲7）には、個人データを入力できる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにするとの記載があるが、これは、望まれる事項の例の中で、「個人データを入力できる端末に付与する機能の、業務上の必

要性に基づく限定」についての例示として挙げられているものにすぎないから、この記載をもって、当然に物理的にパソコンのUSBポートを塞ぐ措置を講ずる注意義務があるということとはできない。

#### イ 内部不正防止ガイドラインについて

確かに、内部不正防止ガイドライン（甲9）では、個人の情報機器及び記録媒体を持ち込まれた場合の情報持ち出しのリスクや、外部記録媒体の業務利用を制限することを対策のポイントとして掲げている。しかし、その中で、具体的な制限の方法についてまで指摘しているわけではなく、内部不正防止ガイドラインの記載から、直ちにUSB接続禁止措置を講ずべき注意義務があるとはいえない。

#### ウ マネジメントシステム実施ガイドラインについて

確かに、マネジメントシステム実施ガイドライン（甲22）では、経済産業分野ガイドラインでの前記アの指摘と同様の指摘がされているが、前記アで説示したとおり、そのことから直ちにUSBポートを塞ぐ措置を講ずべき義務があるということとはできない。

したがって、この点に関する控訴人らの主張は理由がない。

### (3) 情報の書き出し制御措置について

ア 前記認定事実(3)のとおり、被控訴人らが業務用パソコンに本件セキュリティソフトを搭載しており、その設定を変更して、WPDについて接続制御する設定にすれば、業務用パソコンからWPDの一機種であるMTPによる通信方法に対応したスマートフォンに対するデータの書き出しを防止することが可能であり、本件漏えいの方法による情報漏えいは防止できたことが明らかである。そして、被控訴人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、前記(1)及び(2)のお

り、スマートフォンの持込み禁止措置やU S B接続禁止措置を講ずることは、業務従事者に対して過度の制約となり得ること等から被控訴人シンフォームに前記各措置を講ずべき注意義務を認めることはできない中で、書き出し制御措置は実効性があり、かつ、業務従事者に対して必要以上に制約が生じない方法であるから、被控訴人シンフォームにおいて、本件漏えい当時、M T P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いうべきである。

イ これに対し、被控訴人らは、①本件当時、スマートフォンに対する書き出し制御措置を執るべきと明示していたガイドライン等はなく、被控訴人シンフォームの情報セキュリティ対策は十分に高度なものであったこと、②本件セキュリティソフトはM T Pにより通信をするデバイスに対しては読み取りも書き出しも不可とする接続制御機能しか有していなかったのであり、そのような接続制御をすることはパソコンの使用によって得られる利便性を合理的根拠なく放棄するに等しいなどと主張する。

しかし、前記①について、被控訴人シンフォームは、本件個人情報を含む大量の個人情報を扱っていたところ、本件当時、M T Pによる通信方法に対応したスマートフォンによる情報漏えいの危険性を予見することができ、これを回避するための書き出し制御措置をとることができたのであるから、ガイドライン等に記載がなかったことや同様の措置をとっている会社が少なかったとしても、前記認定判断が左右されるものではない。

また、前記②について、被控訴人シンフォームは、本件漏えいが発覚した後、本件セキュリティソフトの設定を変更して、W P Dにつき接続制御機能を有効にする設定に変更したことは、前記認定事実(3)ウ、

エのとおりであって、これによって被控訴人シンフォームの業務に特段の支障を来したという事情もうかがわれないことからすれば、被控訴人シンフォームにおいて、WPDを業務用パソコンに接続させるデバイスとして用いる業務上の必要性があったとは認められず、本件当時、本件セキュリティソフトによりWPDに対する接続制御措置をとることは可能であったといえることができる。

ウ 被控訴人シンフォームは、平成23年8月に本件セキュリティソフトのバージョンアップがされた際に、本件セキュリティソフトの取扱説明書の記載や設定作業を行った販売代理店からの説明等によって、本件セキュリティソフトの設定内容次第であらゆるデバイスの接続制御措置をとることが可能であることを認識することができ、かつ、自らも作業手順を踏むことによって設定内容の変更も可能であったにもかかわらず、平成26年7月に本件漏えいが発覚するまでの間、その設定内容の見直しがされた様子もなく、実際に設定内容の変更はされなかったものである（前記認定事実(3)ウ）。スマートフォンの高機能化が早い速度で進み、自らの情報セキュリティ対策の内容をそれに対応させるために一定程度の時間が必要であることを考慮しても、MTPによる通信方法に対応したスマートフォンであるAndroid 4.0が平成23年10月18日に発売され、その後MTPによる通信方法に対応したスマートフォンの普及率が高まり、これに対応した商用デバイス制御ソフトの製品数も増加していった状況下において、遅くともaが本件個人情報を不正に取得するに至った本件当時（平成25年7月頃から平成26年6月頃）までには、本件セキュリティソフトの設定を見直し、適切な設定内容に変更する注意義務があったといえるべきであり、被控訴人シンフォームにはこれに違反した過失があった

といわざるを得ない。

(4) アラートシステムの設定義務違反について

被控訴人シンフォームは、本件当時、連携システムについてはアラートシステムを設置していたことや、経済産業省の勧告（甲13の2。以下「本件勧告」という。）でも本件データベースについてアラートシステムの対象となっていなかったことが指摘されていることからすると、アラートシステムの設置が情報セキュリティ対策として一定程度有効であった可能性は否定できない。

しかし、情報セキュリティ対策の中には、情報漏えい等の問題を事前に防ぐための対策から、何らかの問題が発生した場合に、その被害を最小限に食い止めるための対策まで、種々のものがあるところ、控訴人らの主張するアラートシステムは、一定量の情報が一度に移動した際に、責任ある立場の者にアラート（警告）が送信され、当該状況に対してどのような対応をすべきかを判断する機会ができるというものであるから、情報漏えいを未然に防ぐことができるわけではない。また、どの程度の量の情報が移動した場合にアラートが発せられる設定とするかによって、それ以下の情報量であればアラートが発せられないことになり、必ずしも情報漏えいの全てを防ぐことができる対策ともいえない。特に、本件においては、被控訴人シンフォームが、本件データベースが保存されているサーバと業務用パソコンとの間の通信量をアラートシステムの対象としていなかったのは、本件システムの開発が終了しておらず、本件システムに種々の不具合が生じており、サーバと業務用パソコンとの間で大量のデータ移動があったため、本件システムの運用開始前に前記通信量をアラートシステムの対象としてしまうことによって本件システムの開発に支障が生じかねないという理由があったこと（甲65）からする

と、前記通信量をアラートシステムの対象にするとしても、アラートが発生する基準値は相当高く設定せざるを得なかったと考えられるのであり、結局のところ、アラートシステムによって、有効に本件個人情報の流出を防止することが可能であったと断ずることはできないというほかない。

そうすると、本件において、控訴人らの主張するアラートシステムを設置したとしても本件漏えいを回避できたとは認められないから、この点に関する控訴人らの主張は理由がない。

(5) 監視カメラ等による監視義務違反について

確かに、情報漏えいの可能性がある執務室内に監視カメラを設置し、従業員等の執務状況を常時監視していれば、情報漏えいの被害が発生したときに、行為者を特定する上で効果があることは否定できない。

しかし、証拠（乙28）によれば、本件漏えい当時、執務室内の全体的な状況を確認できる程度ではあるものの、被控訴人シンフォームの執務室内に監視カメラが設置されていたことが認められるところ、それにもかかわらず本件漏えいを回避することができなかつたものであるから、現に設置されていたものより高精度な監視カメラを設置したとしても、それによって本件漏えいを回避できたのかそもそも疑問であるといわざるを得ない。また、仮に、それをおくとしても、本件個人情報へのアクセス権限を有するaが、本件漏えいの際に、監視カメラで確認することができ、かつ、通常の業務ではしないような行動をしていたのでない限り、現に設置されていたものより高精度な監視カメラの設置によっても本件漏えいを回避できたとは認められないところ、aが、本件漏えいの際に、監視カメラで確認することができ、かつ、通常の業務ではしないような行動をしていたことを認めるに足りる証拠はない。



そうすると、本件において、本件漏えいの行われた執務室内に現に設置されていたものより高精度な監視カメラを設置していたとしても本件漏えいを回避できたとは認められないから、この点に関する控訴人らの主張は理由がない。

#### 4 被控訴人ベネッセの過失責任について

##### (1) 個人情報の利用・管理に責任を持つ部門設置に関する注意義務違反について

前記前提事実5(4)及び証拠（甲3，7，13の1及び2）によれば、経済産業分野ガイドラインにおいて、組織的安全管理措置の項目で、各項目を実践するために講じることが望まれる手法の例示として、「個人情報保護管理者（いわゆる、チーフ・プライバシー・オフィサー（CPO））の設置」が挙げられているところ、被控訴人ベネッセは、本件漏えい以前、同社の法令遵守状況を管理監督する機関としてコンプライアンス部を設け、コンプライアンス部長をCPO（最高個人情報責任者）とし、その下に、専門部署として個人情報保護課を設置し、個人情報保護活動を行っていたこと、経済産業省は、被控訴人ベネッセに対し、平成26年9月26日、同年10月24日までに個人情報保護法20条に基づく安全管理措置及び同法22条に基づく委託先の監督を徹底して、具体的な内容を報告するよう勧告し、勧告の原因として、本件漏えいの対象となったデータベースが、個人情報のダウンロードを監視する情報システムの対象として設定されていなかったところ、被控訴人ベネッセは、被控訴人シンフォームに対して行う定期的な監査において、当該情報システムの対象範囲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同法22条に違反し、被控訴人ベネッセの業務の全過程において同被控訴人の保有する個人情報の利

用・管理に責任を持つ部門を設置せず，その安全管理のために必要かつ適切な措置を講ずることを怠っていたことが同法20条に違反する旨を指摘していることが認められる。

確かに，被控訴人ベネッセにおいて，前記以上に適切な情報管理体制を構築するための組織が本件漏えいの前に存在していれば，情報セキュリティに関する情報を一元的に集約し，より組織的な対応ができた可能性は高まったといえるものの，より組織的な対応ができたからといって，かかる組織が本件漏えいまでにどのような具体的対応をすることができたのかは不明といわざるを得ず，本件漏えいを回避できたとは認められないから，この点に関する控訴人らの主張は理由がない。

## (2) 私物スマートフォンの持込みに関する注意義務違反等について

控訴人らは，被控訴人らは形式上別法人であるが，①被控訴人ベネッセが，元々被控訴人シンフォームの親会社であったものの株式会社ベネッセホールディングスを持株会社とするグループ企業に再編されたことや，②被控訴人シンフォームの役員に被控訴人ベネッセの役員が就任していたことに照らすと，個人情報の管理・運用において，事業としての一体性が見られ，不法行為における責任主体としての一体性が認められると主張する。

しかし，持株会社内の企業間等のいわゆるグループ企業間においては，このような状況は往々にして見られることであり，これらの事実が認められたからといって直ちに，ある法人の過失が他の法人の過失と同視されるものではない。

したがって，被控訴人シンフォームの過失は被控訴人ベネッセの過失と同視できるから被控訴人ベネッセの過失が認められるという控訴人らの主張は，その前提を欠き，理由がない。

(3) 委託先選任及び監督に関する注意義務違反について

ア 委託先選任に関する注意義務違反について

被控訴人ベネッセが、被控訴人シンフォームを委託先として選任したことについて注意義務違反があったことを基礎付ける事実を認めるに足りる証拠はなく、この点に関する控訴人らの主張は理由がない。

イ 監督に関する注意義務違反について

個人情報保護法 22 条は、「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。」と規定し、経済産業分野ガイドライン（甲 7）には、「必要かつ適切な監督」に関し、委託先を適切に選定すること、委託先に個人情報保護法 20 条に基づく安全管理措置を遵守させるために必要な契約を締結すること、委託先における委託された個人データの取り扱い状況を把握することが含まれる旨の記載があり、JISQ 15001（甲 22）は、「3. 4. 3. 4 委託先の監督」において、「事業者は、個人情報の取扱いの全部又は一部を委託する場合は、十分な個人情報の保護水準を満たしている者を選定しなければならない。このため、事業者は、委託を受ける者を選定する基準を確立しなければならない。」、「事業者は、個人情報の取扱いの全部又は一部を委託する場合は、委託する個人情報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。」等と規定し、マネジメントシステム実施ガイドライン（甲 22）は、「審査の着眼点」として、「委託先を選定する基準として、該当する業務については少なくとも自社と同等以上の個人情報保護の水準にあることを客観的に確認できること、

選定基準は具体的で運用可能なものであること」等を例示していることに照らせば、大量の個人情報の運用管理を被控訴人シンフォームに委託していた被控訴人ベネッセには、本件漏えい当時、個人情報の管理について、委託先に対する適切な監督をすべき注意義務があったとすることができる。

そして、前記2で説示したとおり、被控訴人ベネッセも被控訴人シンフォームと同様に、本件当時、本件漏えいの方法による個人情報の漏えいの危険性を予見し得たものであって、被控訴人ベネッセが、被控訴人シンフォームに対し、本件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ていれば、MTPによる通信方法に対応したスマートフォンに対する接続制御機能に対応した設定・変更を指示することができたものであり、このような監督を行うことについて、被控訴人ベネッセに過度の負担が生ずることもなかったと認められる。

そうすると、被控訴人ベネッセには、本件当時、被控訴人シンフォームにおける個人情報の管理につき、本件セキュリティソフトの設定・変更について適切に監督をすべき注意義務があったというべきであり、それにもかかわらず、被控訴人ベネッセは、本件当時、業務用パソコンのセキュリティソフトウェアの変更をすべき旨を指摘することなく放置していた（更新すらされていなかった）結果、本件漏えいを回避できなかったのであるから、前記注意義務に違反したといわざるを得ない。なお、本件勧告においても、被控訴人ベネッセが、被控訴人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同法22条に反すると指摘されていたところで

ある。

以上のとおり，被控訴人ベネッセには，本件当時，被控訴人シンフォームに対する適切な監督をすべき注意義務があり，これを怠った過失があったというべきである。

#### 5 違法な権利侵害の有無について

控訴人らにおいて，本件個人情報につき，自己が開示を欲しない第三者に対してはみだりに開示されたくないと考えることは自然なことであるから，本件個人情報は，控訴人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ものであり，本件漏えいの方法及び被控訴人らの過失行為の内容等に照らし，本件漏えい行為によって，控訴人らは，違法にプライバシーを侵害されたというべきである（最高裁判所平成15年9月12日第二小法廷判決・民集57巻8号973頁，最高裁判所平成29年10月23日第二小法廷判決参照）。

被控訴人らは，本件漏えいに係る行為が，社会通念上許容される限度を逸脱した違法な行為であるとはいえないと主張するが，被控訴人らの過失行為の内容に加え，本件個人情報は，aによって名簿業者に対して売却された上，当該業者から相当多数の企業に売却されたことがうかがわれ，もはやその回収は困難であることを考慮すると，本件漏えい行為に係る被控訴人らの過失行為によって生じた本件漏えいが控訴人らの受忍限度の範囲内にとどまるとはいえない。損害の有無及び程度の検討において被控訴人らの過失行為の内容やその経緯，事後の対応等を考慮する余地はあるとしても，被控訴人らの過失行為が，社会通念上許容される限度を超えておらず，違法性を欠くとはいえない。

#### 6 被控訴人シンフォームの使用者責任について

(1) aについて，本件個人情報を不正に取得してこれを名簿業者に売却

したことにつき、控訴人らのプライバシーを侵害する不法行為が成立することは明らかである。

- (2) 民法715条1項の「ある事業のために他人を使用する者」とは、いわゆる報償責任を認めたとする同法の趣旨に照らせば、広く使用者の指揮・監督の下に使用者の経営する事業に従事する者をいうと解される。

そして、被控訴人シンフォームは、被控訴人ベネッセから委託を受けた業務について、外部の会社に再委託し、同社から更に再々委託を受けた会社の従業員であったaが本件漏えいを行ったものであるところ、被控訴人シンフォームとaの間には雇用関係はなく（争いが無い）、aがシステムエンジニアとして被控訴人シンフォームに派遣され、被控訴人シンフォーム多摩事務所で被控訴人ベネッセの情報システムの開発等の業務に従事していたからといって直ちに、被控訴人シンフォームとaの間に指揮監督関係があったとはいえない。

- (3) 上記の点に関連して、aは、自らの刑事事件において、被控訴人シンフォームから直接指揮命令を受けていたため、被控訴人シンフォーム以下の契約関係は偽装請負であり公序良俗違反により無効であるとの主張をするとともに、被告人質問（甲63、64）において、①所属していたグループでは被控訴人シンフォームの社員であるリーダーから作業を割り当てられ、業務上の指示を受けていたこと、②aが在籍するA社では、雇用契約上、A社の従業員であるTがaを指揮監督する者とされていたが、aの入社後1、2か月が経過した頃にはTとaは別のリーダーの下で作業をするようになり、数か月後にはTの被控訴人シンフォーム多摩事務所への来所が週2、3日程度に減り、その後全く来なくなったりしていたなどの供述をしていたものである

(甲10, 52, 63, 64)。

しかし、上記供述内容を的確に裏付ける客観的証拠は見当たらず、かえって、被控訴人シンフォームにおいて本件システムの開発等の業務に関わっていたb及びfは、aの刑事事件において、再委託先であるA社の従業員についてはA社の従業員である管理者を通じて人員や作業管理を含めた業務上の指揮監督を行っていたという趣旨の証言をしており、実際にそのような指揮監督が行われていたことをうかがわせるメールのやりとりを裏付ける書証(乙114ないし124)も提出されている。aの供述内容は、上記メールのやりとりについては記憶が曖昧であるとし、上記のとおり被控訴人シンフォームのリーダーから直接業務上の指示を受けていた点を強調する一方で、A社の従業員である管理者に対し、被控訴人シンフォームにおける稼働時間の状況報告をしていたことや、自らが不在期間中の業務の代替人員の人選について依頼した可能性があることも供述していることなど一貫しない面があり、仮にTが被控訴人シンフォーム多摩事務所に来所する回数が徐々に減っていった事実があるとしても、システムエンジニアという職務の性質上、逐一相對して指示を受けながら作業をしなければならないとも考えにくいことなどを考慮すると、aの上記供述内容のみから、被控訴人シンフォームとaとの間で実質的な指揮監督関係があった事実を認めることは困難であるといわざるを得ない。

- (4) 控訴人らは、被控訴人シンフォームが、aに対し、被控訴人シンフォームの顧客分析課長等の許可を受けた従業員を通じて業務用アカウントを教示するとともに、業務用パソコンを貸与し、業務開始時の入館証発行に当たっては研修を受けさせ、それ以降、毎年研修を実施していたから指揮監督関係があったとも主張するが、これらの事実が認

められたとしても、aが実際に行っていた業務が、被控訴人シンフォームと受託会社（A社）との間の業務委託契約に基づき受託会社の指揮監督の下に行われていたということと矛盾するものではなく、前記事実から直ちに、被控訴人シンフォームがaの行う業務について具体的に指揮命令をしていたと認めることはできない。

なお、被控訴人シンフォームが、委託先に対し、個人情報保護法上の委託先の監督（同法22条）を行うことがあったとしても、ここにいる監督は、委託先が、委託元との契約に沿って自ら業務を遂行したことに対し、委託元が、委託先の当該業務遂行について当該契約の条項に沿ったものであるか、法令を遵守しているか等をチェックするものであり、委託先の日常の業務を個別具体的に指示するものではなく、使用者責任における指揮監督とは異なるものである。また、被控訴人ベネッセと被控訴人シンフォーム間の業務委託契約において業務の再委託が原則として禁止されていたとしても、上記認定判断を左右するものではない。

したがって、被控訴人シンフォームの使用者責任に関するその余の争点について判断するまでもなく、この点に関する控訴人らの主張は理由がない。

## 7 被控訴人ベネッセの使用者責任について

### (1) 被控訴人シンフォームの使用者としての責任について

被控訴人ベネッセと被控訴人シンフォームとの間の契約は業務委託契約であり（争いが無い）、原則として、受託者が委託者の指揮監督を受ける内容のものではない。被控訴人シンフォームは、従前被控訴人ベネッセにおいて対応していた個人情報等の情報が増加したことに伴い、被控訴人ベネッセからその管理業務の委託を受けたという経緯



に照らせば，被控訴人シンフォームにおいて，専門的知見に基づいて本件システムや本件データベースの運用管理を任されていたと認められ，被控訴人ベネッセから具体的な指揮監督を受けていたとは認められない。また，控訴人らが指揮監督を基礎付ける事実として主張するものは，いずれも個人情報保護法上の委託先の監督を基礎付ける事実とはなり得るが，前記6で説示したとおり，同法上の委託先の監督と使用者責任における指揮監督とは異なるものであるから，これらの事実をもって直ちに使用者責任における実質的な指揮監督関係があったということにはならない。

控訴人らは，持株会社制に移行する以前は，被控訴人シンフォームは，被控訴人ベネッセのシステム部門がそのまま会社になった機能的子会社という位置付けにあり，被控訴人ベネッセに従属する関係にあったなどと主張するけれども，そのような事情を考慮したとしても，上記認定判断を左右するものではない。

したがって，この点に関する控訴人らの主張は理由がない。

(2) a の使用者としての責任について

被控訴人ベネッセと a の間には雇用関係はなく（争いが無い）， a がシステムエンジニアとして被控訴人シンフォームに派遣され，多摩事務所で被控訴人ベネッセの情報システムの開発等の業務に従事していたからといって直ちに，被控訴人ベネッセと a の間に指揮監督関係があったとはいえない。そして，上記(1)のとおり，被控訴人ベネッセが被控訴人シンフォームに対して実質的な指揮監督をしていたとはいえず，また，被控訴人シンフォームが a に対して実質的な指揮監督をしていたともいえないのであって，それらの関係とは別に，被控訴人ベネッセにおいて，被控訴人シンフォームとの間の業務委託契約に

基づく業務の範囲を超えて、直接、a に対して、本件システムの開発に関わる日常業務につき具体的な指示をするなど、実質的な指揮監督関係を及ぼしていたことを裏付ける的確な証拠はなく、控訴人らの上記主張を認めるには足りない。

#### 8 被控訴人らの共同不法行為責任について

前記 2 ないし 5 で説示したとおり、被控訴人シンフォーム及び被控訴人ベネッセは、それぞれ、固有の責任として、控訴人らに対する不法行為責任を負うところ、当該被控訴人らの不法行為は、被控訴人ベネッセが保有し、その管理を被控訴人シンフォームに委託していた本件個人情報の管理に関するものであり、客観的に関連することは明らかであるから、被控訴人らの不法行為は、共同不法行為（民法 719 条 1 項前段）に当たるといえることができる。

#### 9 控訴人らの個人情報の漏えいの有無及び範囲について

(1) 本件漏えいに係る a の行為によって控訴人らの個人情報が漏えいしたか否か及び漏えいした場合の情報の範囲については、当審における当事者らの補充主張も踏まえて以下のとおり補正するほか、原判決の「第 5 当裁判所の判断」の 6 項の(1)ないし(4)に記載のとおりであるから、これを引用する。

(2) 原判決 69 頁 22 行目の「第 1 事件原告 54, 」を削る。

(3) 原判決 72 頁 5 行目の「第 1 事件原告 22 及び」を削る。

(4) 原判決 73 頁 4 行目の末尾の次に、改行して以下のとおり加える。

「控訴人らは、別紙控訴人目録①の控訴人番号 113, 114 の控訴人らについて、上記番号 115 ないし 119 の控訴人らの住所の一部として「c サマカタ」との情報が漏えいしており、上記番号 113 及び 114 の控訴人らの氏のカタカナ表記が漏えいしたものと評価することがで

きるなどと主張する。

しかし、上記事実によって、必ずしも「c」が控訴人番号113, 114の控訴人らの姓であると特定することまではできず、名が漏えいした事実も認められないのであって、上記控訴人らの個人情報に漏えいしたと認めることは困難である（なお、「c」という姓の個人が上記住所地に居住していること自体は住宅地図（株式会社ゼンリン発行）によって既に公開されている（弁論の全趣旨）。）。」

(5) 原判決74頁14行目の冒頭から75頁8行目の末尾までを以下のとおり改める。

「別紙控訴人目録②の控訴人番号12の控訴人については、被保護者である未成年者の情報が漏えいしたことを前提として、上記控訴人が、情報漏えいのお詫びの品として受領した図書券の送付先及び名宛人とされていたことが認められる（甲B12の1及び12の3）。そして、少なくとも上記番号12の控訴人の氏名に関する情報につき、本件漏えいの後に登録されたなどの事実をうかがわせる証拠もないことからすると、上記番号12の控訴人の氏名については、被保護者である未成年者の情報と共に漏えいしたものと推認することができるというべきである。」

(6) 原判決75頁17行目「9,」の次に「12,」を加える。

(7) 原判決76頁13行目の「22,」及び14行目の「30ないし32,」を削る。

(8) 原判決76頁14行目の「37」を「36」に改め、「39,」を削る。

(9) 原判決76頁15行目の「59」を「58」に、「61ないし」を「61, 62,」に改め、「81,」を削る。

(10) 原判決76頁20行目の「193,」を削る。

(11) 原判決 77 頁 7 行目の「54,」, 同 23 行目の「29,」及び「38,」を削る。

(12) 原判決 78 頁 21 行目末尾の次に, 改行して以下のとおり加える。

「(5) 上記認定の氏名が漏えいした控訴人らのうち, 控訴人目録①の控訴人番号 1, 8, 10, 14, 21, 69, 91, 94, 109, 115, 121, 152, 157, 184, 194, 200 及び控訴人目録②の控訴人番号 9, 13, 14, 17 の控訴人らについては, いずれもその被保護者である未成年の控訴人らの保護者としてその氏名(旧姓を含む。)が漏えいしたものであるところ, 証拠(甲 B 13 の 1, B 14 の 1 ないし 3, B 94 の 1 ないし 5, B 157 の 1 及び 2, B 194 の 1 及び 2, B 200 の 1 及び 2) 及び弁論の全趣旨によれば, 本件漏えいが判明した後, 未成年の控訴人らを情報漏えいの対象者とする「お客様情報漏えいに関するご報告およびお詫びの品のご案内」と題する通知書がその保護者である控訴人らに宛てて送付されていることや, 登録者の情報につき, 上記通知書には「サービス登録者」と同時に登録している保護者の情報があったことが認められ, これらの事実によれば, 登録されている保護者の情報は, 未成年者の情報とともに管理されていたと推認することができるので, 保護者である控訴人らの氏名が漏えいされていけば, 氏名のほか, 保護者である控訴人らについても, 被保護者である未成年の控訴人と一般的に共通な情報であるといえる郵便番号, 住所, 電話番号及びファクシミリ番号について, 保護者である控訴人らの情報として漏えいしたとみるのが相当である。」

10 本件漏えいによる控訴人らの損害の発生の有無及びその額について

(1) 本件漏えいによって, 控訴人らの氏名, 性別, 生年月日, 郵便番号,

住所，電話番号，ファクシミリ番号，メールアドレス，出産予定日及び保護者の氏名といった情報が漏えいしたものであるところ，このうち，氏名及び郵便番号・住所，電話番号，ファクシミリ番号及びメールアドレスについては，これらの情報を取得した者において，これらを取得された者に対する連絡が可能となり，また，同情報の使用方法によっては，取得された者の私生活の平穩等に一定の影響が及ぶおそれがある。また，控訴人らがこれらの情報を提供した経緯及び情報の内容に照らし，これらの情報がみだりに第三者への開示がされることはないとの期待が存在したものと考えられ，性別，生年月日，出産予定日及び保護者の氏名も含め，自己の了知しないところで第三者に流出することは欲しないものであったといえることができるから，これらの情報が不正に漏えいした場合には，自己の了知しないところで自己の個人情報情報が漏えいしたことによる私生活上の不安，不快感及び失望感を生じさせたものとして，精神的損害が生じたと認めるのが相当である。

- (2) もっとも，出産予定日を除くこれらの情報は，人が社会生活を営む上で一定の範囲の他者に開示することが予定されている個人を識別するための情報又は個人に連絡をするために必要な情報でもあるため，思想・信条，病歴，信用情報等とは異なり，個人の内面等に関わるような秘匿されるべき必要性が高い情報とはいえない。また，出産予定日については，予定日にすぎないので，秘匿されるべき必要性の程度が相対的に低い。さらに，控訴人らは，本件漏えいでは，控訴人らについて，子供の教育に熱心な，若しくは関心がある親又は教育に熱心な，若しくは関心がある親に育てられた子という属性も流出していると主張するけれども，a はイベントで集めた情報などとして本件個人情報情報を売却しており，情報の量や質から被控訴人らが保有していた情報として漏えいしたことが

推測されていたとしても、これらの属性も、秘匿性が高いものとはいえず、それによって、精神的損害の程度が高まるものということとはできない。

また、本件漏えいに係る情報は、控訴人らそれぞれでその範囲を異にし、その内容も異なるところ、自己の提供した個人を識別するための情報や個人に連絡するために必要な情報を漏えいされたこと自体には違いはなく、その範囲や内容によって、自己の了知しないところで自己の個人情報に漏えいしたことへの不安、不快感等につき、精神的損害の程度を区別して考えるほどの違いがあるとまではいえない。

なお、控訴人らは、未成年の控訴人らに関しては、不安、不快感がこれから一生付きまとうなどして、精神的苦痛は成年者とは異なるとも主張するが、本件漏えいによる影響の期間は、成年者であるか未成年者であるかを問わず、個別の事情によるところが大きい一方、自己の了知しないところで自己の個人情報に漏えいしたことへの不安、不快感の程度は、成年者であるか未成年者であるかは問わず、異なるものとはいえないため、成年原告と未成年原告とで精神的損害の程度を格別に扱う理由までを見いだすのは困難であるので、同主張は採用しない。

- (3) そして、本件漏えいにより、教育関連会社等500社を超える会社に情報が流出したとの報道がされている上、本件漏えいの発覚経緯が、被控訴人ベネッセの顧客から、被控訴人ベネッセに対し、被控訴人ベネッセと異なる通信教育事業者から被控訴人ベネッセに提供していた氏名を名宛人とした書面が送付されているとの指摘が多数寄せられ、しかも、その氏名の中には、被控訴人ベネッセだけに提供していた戸籍上の氏名と異なるものがあるとの指摘が含まれていることに鑑みると、本件漏えいに係る情報も同通信教育事業者に流出した可能性があるといえるもの

の、控訴人らもダイレクトメールやセールス電話が控訴人ら全員に生じているとまでは主張しておらず、前記の流出の可能性を超えて、現時点で、ダイレクトメール等が増えたような気がするという程度以上に財産的損害その他の実害が控訴人らに生じたことはいかなるわけでもない。

一方、被控訴人シンフォームは、aから、個人情報等を漏えいしない旨記載された同意書を取得していたほか、aに対して、情報セキュリティ研修等を受講させていた。そして、被控訴人ベネッセの持ち株会社である株式会社ベネッセホールディングスは、本件漏えいの発覚後に直ちに対応を開始し、情報漏えいの被害拡大を防止する手段を講じ、監督官庁に対する報告及び指示に基づく調査報告を行い、情報が漏えいしたと思われる顧客に対し、本件通知書を送付するとともに、顧客の選択に応じて500円相当の謝罪品の交付を申し出るなどしている。

以上のとおり、本件に現れた一切の事情を総合考慮すると、個人情報の漏えいした控訴人らにつき本件漏えいに係る不法行為によって生じた精神的損害に対する慰謝料として3000円を認めるのが相当である。

そして、控訴人らが控訴人ら訴訟代理人弁護士に本件訴訟の提起及び追行を委任したことは当裁判所に顕著であるところ、その弁護士費用としては、本件事案の難易、請求額、損害額その他諸般の事情を考慮すると、控訴人1人当たり300円の範囲内のものが被控訴人らの不法行為と相当因果関係にある損害とみるのが相当である。

## 11 小括

以上によれば、被控訴人らは、共同不法行為（民法719条1項前段）に基づき、連帯して、別紙控訴人目録①及び②の各控訴人ら（ただし、同目録①の控訴人番号113及び114の各控訴人らを除く。）に対し、同各控訴人らそれぞれにつき3300円及びこれに対する不法行為の以後の

日である平成26年7月7日から支払済みまで民法所定の年5分の割合による遅延損害金の限度で支払義務を負う。

#### 第4 結論

以上によれば、控訴人らの請求をいずれも棄却した原判決は相当でないからこれを変更し、上記の限度で控訴人らの請求を一部認容し、その余の請求をいずれも棄却することとして、主文のとおり判決する。

東京高等裁判所第23民事部

裁判長裁判官 白 石 哲

裁判官 筒 井 健 夫

裁判官 加 本 牧 子