

平成30年12月27日判決言渡 同日原本交付 裁判所書記官

平成27年(ワ)第2486号 損害賠償請求事件 (以下「第1事件」という。)

平成27年(ワ)第2767号 損害賠償請求事件 (以下「第2事件」という。)

平成27年(ワ)第32497号 損害賠償請求事件 (以下「第3事件」という。)

5 口頭弁論終結日 平成30年11月19日

判 決  
主 文

- 1 被告シンフォームは、別紙原告目録の判断欄に○と記載した原告らに対し、  
それぞれ3300円及びこれに対する同原告らのうち第1事件原告及び第3事  
10 件原告については平成26年7月7日から、第2事件原告については同年12  
月9日からいずれも支払済みまで年5分の割合による金員を支払え。
- 2 原告らの被告シンフォームに対するその余の請求及び被告ベネッセに対する  
請求をいずれも棄却する。
- 3 訴訟費用は、①原告らに生じた費用の360分の251、被告シンフォーム  
15 に生じた費用の360分の247及び被告ベネッセに生じた費用の360分の  
255を別紙原告目録の判断番号に1と記載した原告らの負担とし、②原告ら  
に生じた費用の360分の98、被告シンフォームに生じた費用の360分の  
95及び被告ベネッセに生じた費用の360分の101を別紙原告目録の判断  
番号に2と記載した原告らの負担とし、③原告らに生じた費用、被告シンフォ  
20 ームに生じた費用及び被告ベネッセに生じた費用の各360分の1を別紙原告  
目録の判断番号に3と記載した原告の負担とし、④原告らに生じた費用、被告  
シンフォームに生じた費用及び被告ベネッセに生じた費用の各360分の3を  
別紙原告目録の判断番号に4と記載した原告らの負担とし、⑤原告らに生じた  
その余の費用と被告シンフォームに生じたその余の費用は被告シンフォームの  
25 負担とする。
- 4 この判決1項は、仮に執行することができる。

## 事 実 及 び 理 由

### 第 1 請求

#### 1 第 1 事件

被告らは、第 1 事件原告らに対し、連帯して、それぞれ別紙原告目録請求額  
5 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。

#### 2 第 2 事件

被告らは、第 2 事件原告に対し、連帯して、10 万円及びこれに対する平成  
26 年 1 2 月 9 日から支払済みまで年 5 分の割合による金員を支払え。

#### 10 3 第 3 事件

被告らは、第 3 事件原告らに対し、連帯して、それぞれ別紙原告目録請求額  
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

15 本件は、原告らが、通信教育事業等を営む被告ベネッセから委託を受けて原  
告らの個人情報进行分析するシステムの開発、運用等をしていた被告シンフォー  
ムの業務委託先の従業員において原告らの個人情報を外部に漏えいされたこと  
により精神的苦痛を被ったとして、被告シンフォームに対し不法行為又は同従  
業員を被用者とする使用者責任に基づき、被告ベネッセに対し不法行為又は被  
20 告シンフォームを被用者とする使用者責任に基づき、慰謝料等の損害賠償金及  
び不法行為の以後の日である平成 26 年 7 月 7 日（第 2 事件原告については、  
同年 1 2 月 9 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。

#### 1 前提事実

25 以下の事実は、括弧内に証拠を挙げたもの以外は、当事者間に争いがなく、  
又は当事者が争うことを明らかにしない。

- (1) 被告ベネッセは、通信教育、模擬試験や雑誌等の発行・通販事業を行う株式会社である。
- (2) 被告シンフォームは、被告ベネッセのシステム開発・運用を行っている被告ベネッセのグループ会社である。
- 5 (3) 被告ベネッセは、被告シンフォームに対し、平成24年4月頃、顧客の個人情報その他本人の同意を得て取得した個人情報を統合して分析に使用するためのシステム（以下「本件システム」といい、本件システムのデータベースを「本件データベース」という。）の開発・運用・保守の業務（以下「本件業務」という。）を委託した。被告シンフォームは、複数の業者に対し、本件業務の一部を再委託していた。
- 10 (4) Cは、被告シンフォームによる本件業務の委託先の従業員であった。Cは、平成24年4月頃から、被告シンフォームの東京支社多摩事務所（以下「多摩事務所」という。）において、本件データベースにアクセスするためのアカウントの提供を受け、被告シンフォームから貸与を受けた業務用のパソコン（以下、Cが貸与を受けたパソコンを「本件パソコン」といい、被告シン
- 15 フォームが業務従事者に貸与するパソコン一般を「業務用パソコン」という。）を使用し、本件業務に従事していた。
- (5) Cは、平成25年7月頃から平成26年6月27日まで（以下「本件当時」という。）、多摩事務所において、本件パソコンに、本件データベース
- 20 に保管されていた個人情報を抽出して保存した上で、その個人情報を、本件パソコンのUSBポートにUSBケーブルを用いて接続したMTP（メディア・トランスファー・プロトコルのことをいう。以下同じ。）に対応したC所有の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不正に取得した（以下「本件取得行為」という。）。その後、Cは、名簿業者3社に対して、本件取得行為に係る個人情報の全部又は一部を売却した
- 25 （以下、「本件売却行為」といい、本件取得行為と併せて「本件行為」とい

う。)

被告ベネッセは、警察から、Cにおいて名簿業者に売却したとされる個人情報  
情報のデータの提供を受け、これを解析した。その結果では、同データには、  
約2億1639万件の個人情報が記録され、約4858万人分の個人情報が  
5 含まれていた。

[Redacted text block]

10

15

20

(6) MTPは、デジタルカメラの画像転送プロトコルをベースに、音楽・動画  
ファイルなどの転送を可能にした規格であり、音楽・映像プレーヤー等に採  
用されており、デジタルオーディオプレーヤーやデジタルメディアプレーヤ  
ーに音楽ファイルや動画ファイルを転送する目的で設計されている。他方、  
25 USBによるデータ通信に広く利用されているUSBメモリなどの大容量ス  
トレージの通信方法（以下「MSC」という。）では、ストレージ全体をブ

ロック単位で扱い、パソコン側でも操作を行うため、スマートフォンのようなOS（オペレーションシステムのことをいう。以下同じ。）を有するデバイスにおいてMSCによる通信を利用する場合には、パソコン側とデバイス側との双方で操作を行うため不具合が生ずるおそれがある。これに対し、MTPは、ファイル単位での管理を可能とし、パソコン側では操作せず、デバイス側のみで操作をするため、パソコン側とデバイス側との双方で操作を行うために生ずる不具合のおそれがないとの特色を有する。また、MTPは、MTP対応のパソコンでは、ドライバーソフトをインストールすることなく、MTP対応のデバイスとの間で音楽や動画のファイルの相互転送を可能とする特色も有している。

（甲15，16，98の2から4まで）

(7) 別紙情報一覧表（以下「情報一覧表」という。）の「主張・認否」欄（以下、単に「認否欄」という。）のいずれかの情報項目に「○」の記載がある情報がある原告（なお、情報一覧表の原告番号の原告と別紙原告目録の同じ原告番号の原告とは同一である。以下同じ。）について、同情報（ただし、氏名、生年月日、郵便番号及び住所については、別紙原告目録の「氏」「名」欄記載の氏名、同「生年月日」欄記載の生年月日、同「漏えい時郵便番号」欄記載の郵便番号及び同「漏えい時住所」欄記載の住所）は、本件行為により漏えいした。

## 2 当事者の主張

### (1) 原告らの主張

#### ア 原告らの情報の漏えい

平成26年7月7日時点で20歳以上である原告（以下「成年原告」という。）らは、被告ベネッセに対し、自ら又は同日時点で20歳未満である原告（以下「未成年原告」という。）らの保護者として、①氏名、②性別、③生年月日、④郵便番号、⑤住所、⑥電話番号、⑦ファクシミリ番号、

⑧メールアドレス，⑨出産予定日又は⑩未成年原告にあっては保護者の氏名の各情報（ファクシミリ番号，メールアドレス，出産予定日又は保護者の氏名にあっては，認否欄の情報項目に「○」，「▲」，「△」及び「★」のいずれかの記載があるものに限る。）を提供していた（以下「本件個人情報」という。）。本件個人情報（ただし，氏名，生年月日，郵便番号及び住所については，それぞれ，別紙原告目録の「氏」「名」欄記載の氏名，同「生年月日」欄記載の生年月日，同「漏えい時郵便番号」欄記載の郵便番号，同「漏えい時住所」欄記載の住所であり，性別，電話番号，ファクシミリ番号，メールアドレス及び出産予定日については，具体的な内容を特定しない。なお，保護者の氏名は特定されていない。以下同じ。）は，遅くとも同日までに本件行為により外部に漏えいされた（以下「本件漏えい」といい，本件漏えいに係る本件個人情報を「本件漏えい情報」という。）。また，本件漏えいでは，教育事業を営む被告ベネッセの名簿として漏えいされているから，原告らについて，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ている子という属性も漏えいしているといえる。

#### イ 被告らの予見可能性

まず，①「情報システム安全対策基準」（平成7年通商産業省（以下，その後身である経済産業省を含めて，「経産省」という。）告示第518号，平成9年経産省告示第536号による最終改正によるもの。以下「平成9年経産省基準」という。）は，情報システムの機密性を確保することを目的として，故意・過失のリスクを未然に防止するために，情報システムの利用者が実施する対策項目を列挙しているから，個人情報を取り扱う企業にとっての不法行為上の注意義務の基準となる。次に，②「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（平成21年厚生労働省・経産省告示第2号。以下「平成21年経産省ガ

イドライン」という。)は、経済産業分野における事業者等が行う個人情報の適正な取扱いの確保に関する活動を支援する具体的な指針として定められたものであり、個人情報の保護に関する法律(平成15年法律第57号。以下「個人情報保護法」という。)が事業者に対し個人の情報の取扱いに関し義務を課すことで各人の権利を保護しているため、個人情報保護法が定める義務が不法行為上の注意義務を構成するといえる。また、③独立行政法人情報処理推進機構の平成25年3月25日作成の「組織における内部不正防止ガイドライン」(以下「平成25年IPAガイドライン」という。)は、企業等において必要な内部不正対策を効果的に実施可能とするを目的とするため、平成25年IPAガイドラインで要求する事項を考慮しない場合には、不法行為上の注意義務違反となるというべきである。さらに、④日本工業標準調査会の平成18年策定の「個人情報保護マネジメントシステム—要求事項(JIS Q 15001:2006)」(以下「JIS基準」という。)は、事業者が業務上取り扱う個人情報を安全で適切に管理するための標準となるべく策定された日本工業規格であり、財団法人日本情報処理開発協会(当時)の平成22年9月17日発行の「JIS Q 15001:2006をベースにした個人情報保護マネジメントシステム実施のためのガイドライン 第2版」(以下、「平成22年JISガイドライン」といい、JIS基準と併せて「JIS基準等」という。)は、JIS基準により個人情報保護マネジメントシステムを構築し、運用するためのガイドラインであるため、JIS基準等で要求されている事項を満たさない場合には、業務上個人情報を取り扱う事業者に要求される水準を満たさないものとして、不法行為上の注意義務違反となる。加えて、⑤日本データセンター協会の平成25年8月28日作成の「データセンター セキュリティ ガイドブック Ver1.0」(以下「平成25年データセンターガイドブック」という。)は、データセ

センターの適切なセキュリティに関する理解を深め、日本のデータセンターの活用のために広く参照されることを目標として、適切なセキュリティを考えるために必要なものを示すものである。当該基準は、個人情報を取り扱う企業にとっての注意義務の指標となる。そして、上記の基準やガイドライン等の内容などからすると、個人情報を取り扱う事業者にとって、本件当時、外部記録媒体へ格納する方法による情報漏えいのリスクや、これを防止するための対策の必要性等が広く認識されている状況にあった。

また、被告シンフォームは、毎年、実施する社員及び業務委託先の従業員の全員を対象とする情報セキュリティ研修において、顧客の個人情報の大量持ち出し事例の紹介やスマートフォンを含む外部記録媒体への書き出し制御を実施している旨を周知していたので、スマートフォンが外部記録媒体として機能することやスマートフォンへ本件個人情報を書き出す手法による情報漏えいのリスクを十分に把握していた。

さらに、被告シンフォームでは、本件業務に従事する複数の業務従事者が共用するアカウントの教示を受けた従業員において、業務用パソコンから本件データベースにバッチサーバ経由でアクセスすることで、個人情報にアクセスし、スマートフォン等に個人情報を書き出すことは容易であった。

他方、アンドロイドをOSとするスマートフォン端末（以下「アンドロイドスマートフォン」という。）のうち、MTPに対応したバージョン4.0以降のもの（以下「アンドロイド4.0」という。）は、平成25年4月には、少なくとも1235万台を超えて使用されていた。

そうすると、被告らはスマートフォンを記憶媒体として利用した不正行為の可能性を認識することが可能であった。

したがって、被告らには、本件当時、業務用パソコンにアクセスを有する者において、業務用パソコンにスマートフォンをUSBケーブルにて接

続し、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の予見可能性があった。

#### ウ 被告シンフォームの注意義務

##### (ア) 持込禁止義務

5 被告シンフォームは、被告ベネッセの顧客の大量の個人情報を取り扱っており、その個人情報の中には、子供に関する個人情報も多く含まれる。特に子供に関する個人情報は、漏えいした場合の影響が長時間に及ぶなど悪影響が甚だしく、同情報を大量に保有し、管理している企業には、個人情報が漏えいしないように最大限の配慮が求められる。

10 また、平成9年経産省基準では「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」と明記され、平成25年IPAガイドラインでも個人所有の記録媒体の業務フロア内への持込みを制限することを対策のポイントとして挙げ、さらに、平成25年データセンターガイドブックにも記録媒体の持込み制限をセキュリティ対策として挙げていることからすると、個人情報を取り扱う事業者においては、  
15 本件当時、情報漏えいの防止対策として、記録媒体の持込みを禁止する方法が広く認識されている状況にあった。

そして、私物のスマートフォン等を業務上利用する必要はなく、この持込みを制限することは、コストも手間も掛からない。

20 したがって、被告シンフォームは、業務委託先の従業員に対し、本件当時、私物スマートフォン等の業務エリアへの持込みを禁止する措置を講ずるべき注意義務（以下「持込禁止義務」という。）を負っていた。

それにもかかわらず、被告シンフォームは、本件当時、私物スマートフォン等の業務エリアへの持込みを禁止していないので、持込禁止義務  
25 に違反している。

##### (イ) USB接続禁止義務

被告シンフォームは、前記(ア)のとおり、大量で、センシティブな情報を扱っているため、本件個人情報漏えい防止のために最大限の配慮が求められる。

5 平成21年経産省ガイドラインでは「個人データを入力できる端末」において「外部記録媒体」を接続することができないようにすることが望ましいとの記載がされ、平成25年IPAガイドラインでは外部記録媒体の業務利用の制限を対策のポイントに挙げ、平成22年JISガイドラインでは外部記録媒体を接続することができないようにすることを業務上の必要性に基づく対策として挙げていることからすると、個人情報  
10 情報を取り扱う事業者において、本件当時、情報漏えいの対策として、業務用パソコンに記録媒体を接続することができないようにする方法が広く認識されている状況にあった。

他方、USBポートを物理的に塞ぐ器具は、遅くとも平成17年には発売され、情報漏えい対策として一般的なものとなっていた。そして、  
15 USBポートを物理的に塞ぎ、又は少なくとも接続を禁止するルールを設けることは、コストも手間も掛からない。他方、マウスの接続はUSB以外の方法でも可能であり、あらかじめ固定して外せないようにすることも可能であり、また、顧客等へのデータ提供についても、必要に応じて一時的に上司等の立会いの下、USBメモリの接続を認めれば業務  
20 に支障はなかった。そうすると、被告シンフォームにおいて、USB接続（USBポートにUSBケーブルを用いて接続することをいう。以下同じ。）を禁止することは可能かつ容易であった。

したがって、被告シンフォームは、本件当時、業務用パソコンにUSB接続を禁止する措置を講ずるべき注意義務（以下「USB接続禁止義務」という。）を負っていた。  
25

それにもかかわらず、被告シンフォームは、本件当時、USB接続を

禁止する措置を講じていないので、USB接続禁止義務に違反している。

(ウ) 書き出し制御義務

5 被告シンフォームは、前記(ア)のとおり、大量で、センシティブな情報を扱っているので、本件個人情報漏えいしないように最大限の配慮が求められる上、平成25年IPAガイドラインでは、個人の情報機器及び記録媒体が持ち込まれた場合のリスクを具体的に指摘している。

10 そして、商用デバイス用のセキュリティソフトウェア（以下「セキュリティソフト」という。）では、平成19年7月から平成25年8月にかけて、MTPに対応しており、また、平成24年夏以降に発売されたアンドロイドスマートフォンは、全てアンドロイド4.0のMTP通信  
15 に対応する端末であり、相当程度市場に出回る見通しであったから、それを予測することができる時点で、その対策が当然に必要となるというべきである。

20 他方、業務用パソコンにMTPの使用制御（パソコンからデバイスへのデータの書き出しを制御することをいう。以下同じ。）又は接続制御（同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ことをいう。以下同じ。）の機能に対応したセキュリティソフトを搭載することは、個人情報漏えいの対策に極めて有効で、これを採ることは可能かつ容易であった。

25 したがって、被告シンフォームは、本件当時、業務用パソコンにMTP使用制御又は接続制御の機能に対応したセキュリティソフトを搭載することにより、情報の書き出しを制御し、又は機器の接続を制御する措置を講ずるべき注意義務（以下「書き出し制御義務」という。）を負っていた。

30 それにもかかわらず、被告シンフォームは、本件当時、本件セキュリティソフトでは、MTP通信による情報の書き出しを制御しておらず、

また、MTPに対応した機器の接続を制御していないので、書き出し制御義務に違反している。

(エ) アラート設定義務

5 被告シンフォームは、前記(ア)のとおり、大量で、センシティブな情報を扱っているので、本件個人情報漏えいしないように最大限の配慮が求められる上、平成25年IPAガイドラインでは、個人の情報機器及び記録媒体が持ち込まれた場合のリスクを具体的に指摘している。

10 そして、被告らも、本件漏えいの発覚直後から、再発防止策の緊急対策としてアラート機能を設定することを一番目の項目として挙げ、また、被告ベネッセが経産省に対する最終の事故調査報告書においてアラートシステムが機能しなかったために本件行為を防止することができなかつた旨記載しているように、被告らは、アラートシステムを設定しておけば、従業員に対する警告となると考えていた。

15 したがって、被告シンフォームは、本件当時、本件データベースと業務用パソコンとの間に通常業務における以上の通信量が認められた場合に管理者に対してメール等により警告が発せられ、管理者がそれを許容するかを確認するシステムを設定すべき注意義務（以下「アラート設定義務」という。）を負っていた。

20 それにもかかわらず、被告シンフォームは、本件当時、上記アラートシステムを設定していないので、アラート設定義務に違反している。

(オ) 監視カメラ設置義務

被告シンフォームは、前記(ア)のとおり、大量で、センシティブな情報を扱っているので、本件個人情報漏えいしないように最大限の配慮が求められる。

25 平成25年IPAガイドラインでは「重要情報を扱う物理的区画」のセキュリティ強化としてカメラ等で監視する旨やその監視をしているこ

5 とを伝える旨が記載され、また、平成25年データセンターガイドブックでも実施されるセキュリティ対策として画像監視システムを挙げていることからすると、個人情報を取り扱う業者において、本件当時、情報漏えいの対策として、情報を扱う執務室の監視カメラ等による監視の必要性が広く認識されている状況にあった。

10 また、個人情報を取り扱う作業スペースに監視カメラを設置し、常時行動を監視した場合、従業員が同スペースで不正行為に及ぶことを抑止することができ、また、監視カメラにより行動を監視していれば速やかに情報漏えいに対処することが可能であり、個人情報の拡散を抑制することができる。他方、被告シンフォームでは、情報漏えいのリスクを十分に認識して、主要な入退出口には防犯カメラを設置していたように、防犯カメラを設置することは容易であった。

15 したがって、被告シンフォームは、本件当時、監視カメラにより執務室を監視し、それを従業員等に伝えるべき注意義務（以下「監視カメラ設置義務」という。）を負っていた。

それにもかかわらず、被告シンフォームは、本件当時、監視カメラにより執務室を監視せず、また、監視カメラにより執務室を監視していることを従業員等に伝えていないので、監視カメラ設置義務に違反している。

20 エ 被告ベネッセの注意義務

(ア) 部門設置義務

25 個人情報保護法が定める義務は、前記イのとおり、不法行為上の注意義務を構成するところ、個人情報保護法20条では、個人情報を取り扱う事業者個人データの安全管理のために必要かつ適切な措置を講ずることを義務付け、平成21年経産省ガイドラインは、義務的事項として、個人データの安全管理措置を講ずるための組織体制の整備を挙げ、また、

平成25年IPAガイドラインも組織横断的な管理体制の構築を求めている。

5 また、個人情報を取り扱うに当たり、利用・管理に責任を持つ部門が存在しない場合には、保有する情報を統括して管理することができず、個人情報の取扱いや管理が杜撰となり、情報の漏えいが生じる可能性が高まる。そして、被告ベネッセの事業規模からすると、同部門を設置することは可能かつ容易であった。

10 さらに、被告ベネッセが取得した個人情報は、大量で、センシティブな情報が含まれている上、被告シンフォームに本件システムの構築を委ね、更に被告シンフォームが委託先にその一部を委託するなど、被告ベネッセの顧客情報に接触する者が被告ら以外の会社の従業員を含め多岐にわたっていた。そして、後記(ウ)のとおり、被告ベネッセには個人情報を取り扱う委託先に対して必要かつ適切な監督を行う義務等があった。

15 したがって、被告ベネッセは、本件当時、保有する個人情報の利用・管理に責任を持つ部門を設置すべき注意義務（以下「部門設置義務」という。）を負っていた。

それにもかかわらず、被告ベネッセは、本件当時、実質的に、保有する個人情報の利用・管理に責任を持つ部門を設置していないので、部門設置義務に違反している。

20 (イ) シンフォーム同様義務

被告ベネッセは、被告シンフォームに本件業務を委託しているものの、元々被告シンフォームの親会社であったものが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経緯及び被告シンフォームの役員に自社の役員を就任させていた状況等から、実質的には、被告シンフォームを自社の一部門と同様の状態で事業を行っていた  
25 ということができる。

そうすると、被告ベネッセは、被告シンフォームと一体となり、組織的な事業として本件システムの開発・運用を行い、組織的に一体として本件個人情報を取り扱っていたと評価することができる。

5 したがって、被告ベネッセは、本件当時、前記ウの被告シンフォームの注意義務と同様の持込禁止義務、USB接続禁止義務、書き出し制御義務、アラート設定義務及び監視カメラ設置義務の各注意義務（以下「シンフォーム同様義務」という。）を負っていたと評価することができる。

10 それにもかかわらず、被告ベネッセは、本件当時、シンフォーム同様義務を果たしていないので、シンフォーム同様義務に違反している。

#### (ウ) 委託先選任監督義務

15 個人情報保護法22条は、個人情報を取り扱う事業者は、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旨規定しているところ、被告ベネッセは、被告シンフォームに本件業務を委託しているため、被告シンフォームに対する必要かつ適切な監督を実施する義務を負っていた。そして、平成21年経産省ガイドラインは、必要かつ適切な監督に、委託先を適切に選択すること、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及び委託先における委託された個人データの取扱い状況を把握することを含めている。しかも、被告ベネッセが取得した個人情報は、前記(ア)のとおり、大量で、センシティブな情報が含まれている。

25 したがって、被告ベネッセは、本件当時、業務委託先を選任する当たり、適切に個人情報を管理する体制にある業者を選任すべき注意義務及び個人情報保護法20条に基づく安全管理措置が委託先で適切に採ら

れているかを監督するべき注意義務（以下「委託先選任監督義務」という。）を負っていた。

それにもかかわらず，被告ベネッセは，本件当時，適切に個人情報管理する体制にある業者を選任せず，また，個人情報保護法20条に基づく安全管理措置が委託先で適切に採られていることを監督していないので，委託先選任監督義務に違反している。

#### オ 被告らの行為の違法性

本件個人情報は，無制限な開示，保有，利用が許される情報でなく，法的保護の対象となる上，本件行為には，何らの正当な理由がない。

したがって，本件行為は，原告らのプライバシーを侵害し，違法である。

#### カ 被告シンフォームのCを被用者とする使用者責任

(ア) Cは，原告らが名簿業者に本件個人情報を提供することを許諾していないことを知りながら，本件行為により，故意に原告らのプライバシーを侵害しており，原告らに対して，本件行為につき不法行為に基づく損害賠償責任を負う。

(イ) 本件取得行為は，Cが多摩事務所において，本件業務を行う際にされており，また，本件売却行為は，本件システムの開発等の業務従事行為を契機として，これと密接な関連を有した行為である。

したがって，本件行為は，被告シンフォームの「事業の執行について」されたものに当たる。

(ウ) 民法715条の使用関係は，実質的な指揮監督関係があれば足りるところ，Cは，被告シンフォームの社員であるグループリーダーから，多摩事務所において，グループの一員として個別の業務を割り当てられ，直接指示を受け，また，被告シンフォームから，業務用アカウントを教示され，本件パソコンを貸与され，研修を受講させられてきた。

したがって，被告シンフォームは，Cを実質的に指揮監督する関係に

あった。

(エ) なお、被告シンフォームは、Cの選任及びその事業の監督について相当の注意をしていない。

5 (オ) よって、被告シンフォームは、原告らに対し、本件行為につきCを被用者とする使用者責任に基づく損害賠償責任を負う。

キ 被告ベネッセの被告シンフォームを被用者とする使用者責任

(ア) 被告シンフォームは、前記ウのとおり、持込禁止義務、USB接続禁止義務、書き出し制御義務、アラート設定義務及び監視カメラ設置義務の各違反により不法行為責任を負う。

10 (イ) また、本件業務は、被告ベネッセの商品・サービス開発やマーケティングのためのものであるので、被告シンフォームの前記(ア)の各違反行為は、被告ベネッセの「事業の執行について」されたものに当たる。

(ウ) 被告ベネッセは、被告らの属するグループの組織体制において、被告シンフォームの上位にあり、被告シンフォームに指示を出す立場にあり、  
15 被告シンフォームに、同グループにおいて最も重要な経営基盤と位置付けられた本件システムの開発を行わせ、仕様を指示し、その進捗を管理し、被告ベネッセの管理職の社員を被告シンフォームの従業員に兼務させ、被告ベネッセの社員において被告シンフォームの社員や委託先の従業員に対し、直接指示をするなどしていた。

20 したがって、被告ベネッセは、本件業務について、被告シンフォームを実質的に指揮監督する立場にあった。

(エ) なお、被告ベネッセが被告シンフォームの選任及びその事業の監督について相当の注意をしていない。

(オ) よって、被告ベネッセは、原告らに対し、本件行為につき被告シンフォームを被用者とする使用者責任に基づく損害賠償責任を負う。  
25

ク 原告らの損害

5 本件個人情報、基本的な個人情報であるが、高度情報化社会においては、情報の保存、検索、連結、解析が技術的、費用的に可能となり、住所、生年月日などはそれ自体重要な意味を持つようになり、重大な価値を有している上、センシティブな情報で、入手を欲する者にとっては、高い経済的価値を持つ一方、漏えいされた者からすれば、通常開示を欲しない情報である。また、本件個人情報の流出先は、約500社に上り、流出の範囲は広く、回収が困難である上、流出先からの再流出の懸念も大きい。

10 そして、成年原告には、ダイレクトメール、電子メール及び勧誘の電話を受けるとの具体的な被害を受けている者がいるほか、不特定の者によって本件個人情報が購入され、その回収が不可能であるため、いかなる目的で何時利用されるか分からないという不安感・不快感を抱いており、訪問勧誘や電話勧誘等も迷惑である。他方、未成年原告は、これらと同様の事情に加え、同不安感・不快感に一生付きまとい、学校の入学・卒業・受験など多くの場面で業者に利用されるだけでなく、犯罪等への利用も警戒  
15 しなければならず、親の情報が一緒に漏えいしている場合には悪用される危険度が更に高まるので、不快感による精神的苦痛が成年の比ではない。

したがって、本件行為による精神的苦痛は、成年原告（第2事件原告を除く。）が4万5000円（第2事件原告にあつては9万5000円）を下らず、未成年原告が9万円を下らない。

20 また、本件は個人情報漏えいという高度に複雑な事柄に関するため、原告らは、法律専門家である弁護士に法的手続を依頼せざるを得ないので、本件訴訟の弁護士費用のうち、本件行為による不法行為と相当因果関係のある損害としては、成年原告につき1人当たり5000円、未成年原告につき1人当たり1万円が相当である。

25 ケ 以上によれば、被告らは、不法行為又は使用者責任に基づく損害賠償責任を負い、被告シンフォームにおいて被告ベネッセの個人情報の管理を受

託していたので、原告らに対し、共同で安全管理措置を徹底する義務を有していたから、被告らには共同不法行為が成立する。

(2) 被告らの主張

ア 原告らの情報漏えいについて

5 (ア) コード判明原告について

情報一覧表の「登録コード」欄に登録コード（被告らが本件行為の後に本件行為に係る情報漏えい対象者ごとに付している管理番号をいう。以下同じ。）の記載があり、かつ、情報一覧表の「コード帰属者」欄が空欄となっている原告ら（以下「コード判明原告」という。）においては、①認否欄の情報項目に「▲」の記載がある情報については、同認否欄の「備考」欄に記載の理由により漏えいした情報の内容と原告らの主張する情報の内容が一致せず、②認否欄の情報項目に「△」の記載がある情報については、当該情報の漏えいがあったことは認めるものの、性別、電話番号、ファクシミリ番号、メールアドレス及び出産予定日については、原告らが具体的内容を主張しないため、その内容を知らず、③認否欄の情報項目に「★」の記載がある情報の漏えいがあったことは、  
10 否認し、又は知らない。

(イ) コード帰属未定原告について

情報一覧表の「登録コード」欄に登録コードの記載があり、かつ、同  
20 「コード帰属者」欄に「不明」と記載されている原告ら（以下「コード帰属未定原告」という。）については、本件個人情報が漏えいしたことは知らない。

なお、コード帰属未定原告に係る情報一覧表記載の登録コードが当該  
コード帰属未定原告のものであった場合には、当該コード帰属未定原告  
につき、①認否欄の情報項目に「▲」の記載がある情報については、備  
25 考欄に記載したとおりの理由により正確な情報が漏えいしておらず、②

認否欄の情報項目に「△」の記載がある情報については、当該情報に関する漏えいがあったことを認めるものの、漏えいした情報の内容は知らず、③認否欄の情報項目が「★」の記載がある情報の漏えいがあったことは、否認し、又は知らない。

5 (ウ) コード不明原告について

情報一覧表の「登録コード」欄に登録コードの記載がない原告ら（以下「コード不明原告」という。）の本件個人情報の漏えいがあったことは、否認し、又は知らない。

イ 被告らの予見可能性について

10 まず、①平成21年経産省ガイドラインは、個人情報保護法が予防的に一定の名宛人に公法上の安全管理措置義務を定めて個人情報を保護するものであり、個人情報を個人の権利利益と位置付けるものでなく、また、個人情報保護法上求められる安全管理措置を採らなかったとしても、それが直ちに不法行為上の注意義務違反となるものではない。

15 また、②平成9年経産省基準は、サーバールームやデータセンターにおけるセキュリティ対策に係る基準であり、通常企業の執務室における情報セキュリティ対策に当てはめることは不相当であり、情報システムに関する技術やこれを取り巻く環境が本件当時とは異なっており、③平成25年IPAガイドラインは、組織における内部不正を防止するためのノウハウ集にすぎず、違法とはいえない行為も対象に含めて防止策を提示するものであり、さらに、④JIS基準等は個人情報保護法の要求事項を超えた高い保護レベルを前提としており、⑤平成25年データセンターガイドブックは、企業の執務室における情報セキュリティ対策の基準としては不相当であり、いずれも、個人情報保護法との関係で法規範性を有することは  
20  
25 なく、不法行為上の注意義務の内容や範囲を画するものではない。

アンドロイド4.0が平成23年10月18日にリリースされ、MTP

通信によりウィンドウズパソコンとアンドロイドスマートフォンとで相互に情報通信ができることとなったところ、本件当時まで、パソコンからM T P通信によりスマートフォンにデータが書き出されることによる情報流出の危険性やその対策を採ることの必要性について、社会的に認識されておらず、M T P通信に対する情報流出につき従来のM S Cデバイス制御の技術的措置とは異なる対策を採らなければならないといった問題認識が社会的になかった。また、被告らにおいて、本件当時まで、業務用パソコンからスマートフォンに書き出しがされ、外部に情報が持ち出されたなどのM S Cデバイスの書き出し制御措置が機能しない事態があることを疑わせる事故等が発生したことがなく、そのような疑いをもつ契機がなかった。

したがって、被告らは、本件当時、業務用パソコンにアクセスをする権限を有する者において、業務用パソコンにM T P対応のスマートフォンをU S Bケーブルにて接続し、M T P通信でデータを転送する方法によって個人情報をも不正に取得することの予見可能性があったとはいえない。

#### 15 ウ 被告シンフォームの注意義務について

##### (ア) 持込禁止義務について

まず、保管されている個人情報の量によって、採るべき安全管理措置の水準が異なる理由はない。

原告らの指摘する平成9年経産省基準、平成25年I P Aガイドライン及び平成25年データセンターガイドブックの記載は、被告シンフォームの注意義務を根拠付けるものとはならない。他方、私物スマートフォン等の持込み禁止は、平成21年経産省ガイドラインでは、義務的事項としても、望ましい事項ともされておらず、また、本件当時、一般の企業において、例外的な場合を除き採用されていないのみならず、本件当時の後も、プライバシーマークやI S M S認証（情報セキュリティに関する国際規格の1つであるI S M S認証基準に適合していることにつ

いての第三者機関による認証をいう。以下同じ。)を取得しようとする企業でも、標準的に採られている措置とはされていなかった。

5 さらに、私物スマートフォンの持込みを禁止することは、これを徹底しない限り実効性がない一方、これを徹底すると業務を著しく阻害するので、現実的ではない。

したがって、被告シンフォームは、本件当時、持込禁止義務を負っていたとはいえない。

(イ) U S B 接続禁止義務について

10 原告らの指摘する平成21年経産省ガイドラインの該当部分は、「個人データを入力できる端末」すなわち個人データを入力することのみを目的とする端末について「外部記録媒体」を対象とするものであるのに対し、本件パソコンは、個人データの一時記録も含め広く開発及び運用業務に使用されていたので、当該端末に該当せず、また、スマートフォンは、「外部記録媒体」とは異なるものとして扱われていたので、平成  
15 21年経産省ガイドラインは、U S B 接続の禁止につき、義務的事項としていないのみならず、望ましい事項としていない。原告らが指摘する平成25年I P Aガイドラインや平成22年J I Sガイドラインの記載は、被告シンフォームの注意義務を根拠付けるものとはならない。

20 また、本件当時、業務上利用するパソコンに対するU S B 接続禁止措置を採っている企業は少なかったのみならず、本件当時の後においても、プライバシーマークやI S M S 認証を取得しようとする企業でも、同措置を採っている会社は数パーセント程度しかなく、その他ほとんどの企業では同措置を採っていないので、同措置は標準に採られている措置ではなかった。

25 さらに、U S B ポートを物理的に塞ぐ器具は取り外し可能であり、また、パソコンには、マウス、キーボード及び業務上利用するU S B など

を接続するためのUSBポートが必要であるため、全てのUSBポートを塞ぐものではないので、USBポートを塞ぐことは、本件漏えいにとって有効な対策とならない。

5 したがって、被告シンフォームは、USB接続禁止義務を負うとはいえない。

(ウ) 書き出し制御義務について

原告らの指摘する平成25年IPAガイドラインは、情報書き出し制御措置に言及しておらず、情報書き出し制御措置は高度な対策であり、一般の企業に求めることは現実的でなく、本件当時、プライバシーマークやISMS認証を取得しようとする企業でも、過半が書き出し制御措置を採っておらず、書き出し制御措置は標準的に採られている措置ではない。まして、書き出し制御措置を採っている少数の企業でも、MTP通信まで対象としていたものはほとんどなかったもので、MTP通信までの書き出し制御措置は標準的に採られている措置となっていない。

15 また、被告シンフォームは、平成17年から、業務用パソコンに、外部記憶媒体に情報を書き出すことを制限する本件セキュリティソフトを搭載していたところ、本件行為が発覚するまで、MTP対応のスマートフォンのリスクについては、情報セキュリティの専門家においてもほとんど認識されておらず、注意喚起等もされておらず、被告シンフォーム  
20 において、業務用パソコンから外部記録媒体に書き出しが制御されていないことを疑わせる事故等がなく、また報告がされることもなかった。

したがって、被告シンフォームは、書き出し制御義務を負うとはいえない。

(エ) アラート設定義務について

25 原告らの指摘する平成25年IPAガイドラインは、情報持ち出しのリスクに対する対策としてアラートシステムの設定を指摘しておらず、

アラート設定義務があることを認める根拠とはならない。そして、平成  
21年経産省ガイドラインは、アラートシステムの設定につき、義務的  
事項とも、望ましい事項ともしていない。

5 また、本件当時、高度な情報セキュリティ対策を採っている企業でも、  
アラートシステムを採用している企業は少数で、本件当時の後において  
も、プライバシーマークやISMS認証を取得しようとする企業でも、  
アラートシステムを採用していないものが大半であって、アラートシス  
テムは標準的に採られている措置ではなかった。

10 しかも、アラートシステムは、正当な業務による通信であっても、設  
定された条件を満たせば、自動的にアラートが発令される仕組みである  
ため、その対象を広範に設定すれば、頻繁にアラートが発せられ、日常  
業務に支障が生じ、運用に堪えないものとなる一方、意図的に不正を働  
く場合、複数回に分割してダウンロード等を行うことで、予想される基  
準値を超えないようにすることが容易であるので、情報漏えい対策とし  
15 ての実効性に乏しい。Cの取り扱う日常のデータ量は相当程度大きい  
ので、Cの業務上通常必要とされる量を超える値はかなり高い基準値とな  
るのに対し、個人情報のデータ量は小さいから、本件取得行為の際に、  
業務上通常必要とされる量を超える値よりも高かったということはでき  
ない。

20 したがって、被告シンフォームは、アラート設定義務を負うとはいえ  
ない。

なお、仮にアラートシステムが設定されていたとしても、警告だけで  
は、情報の不正取得行為によりアラートシステムが発令されたときは既  
に同通信が行われた後であるという関係から、アラート設定義務の違反  
25 と本件行為との間に相当因果関係があるとはいえない。

(オ) 監視カメラ設置義務について

原告らが指摘する平成25年IPAガイドラインの「重要情報を扱う物理的区画」は、従業員が日常執務をする執務室を想定しているとはいえず、その内容も対策のヒントにすぎないので、監視カメラ設置義務の根拠とはならず、平成25年データセンターガイドブックは、執務室の情報セキュリティ対策のものとしては不相当であるので、被告らの注意義務の根拠とはならない。そして、平成21年経産省ガイドラインは、監視カメラの設置につき、義務的事項とも、望ましい事項ともしていない。

また、本件当時、高度な情報セキュリティ対策を採っている企業でも、執務室内に監視カメラを設置している企業は少数で、本件当時の後においても、プライバシーマークやISMS認証を取得しようとする企業でも、執務室内に監視カメラを設置しないものが大半であって、執務室内における監視カメラの設置は標準的に採られている措置ではなかった。

しかも、監視カメラは、常時、監視員が監視していなければ不審な動きが見られた時点でそれを把握することは不可能で、また、執務室内で従業員が通常の業務をしているのか、不正に情報の閲覧や保存等をしているのかは外形的に分からないので、業務用パソコンから情報の不正取得を防止するために監視カメラを設置することの実効性はない。他方、執務室内における監視カメラの設置は、従業員に対し、不快な思いを生じさせかねず、プライバシー侵害などの問題視がされるおそれもある。

したがって、被告シンフォームは、監視カメラ設置義務を負うとはいえない。

なお、被告シンフォームは、執務室内に監視カメラを設置したので、監視カメラ設置義務に違反していない上、仮に監視カメラを設置していたとしても、本件取得行為において、Cの挙動に外形上不審なものはなく、通常の執務態度であったから、本件取得行為を抑止することはでき

ず、監視カメラ設置義務の違反と本件取得行為との間に相当因果関係があるとはいえない。

エ 被告ベネッセの注意義務について

(ア) 部門設置義務について

5 個人情報保護法が個人情報取扱事業者に対して主務大臣との関係で顧客情報の利用・管理に責任を持つ部門を設置すべきことを義務付けているとしても、同部門を設置することが不法行為上の注意義務となるとはいえず、また、個人情報保護法上、個人データの安全管理措置を講ずるための組織体制の整備が義務付けられているとしても、個人情報の利用  
10 ・管理に責任を持つ部門を設置することまでは義務付けられていない。

したがって、被告ベネッセは、部門設置義務を負うとはいえない。

なお、被告ベネッセは、個人情報保護の最高責任者として最高個人情報責任者を選任し、その下に、個人情報保護活動を推進する専門部署として、個人情報保護課を設置していた。

15 また、被告ベネッセが個人情報の利用・管理に責任を持つ部門を設置しないことと、被告シンフォームに対する適切な監督を妨げ、被告シンフォームの不十分な情報管理体制を放置したこととは具体的な因果の流れが明らかでないので、部門設置義務の違反と本件行為の間には相当因果関係があるとはいえない。

20 (イ) シンフォーム同様義務について

法人格が異なる者について別個独立の権利義務の主体として取り扱うことは、我が国の法の基本であり、例外的に、厳格な要件のもと法人格否認の法理により法人格が否認されることがあるにすぎない。原告らが主張する事情は、我が国のグループ企業内では普通のもので、これによ  
25 って法人格が否認されることはない。

したがって、被告ベネッセは、シンフォーム同様義務を負うとはいえ

ない。

(ウ) 委託先選任監督義務について

5 被告シンフォームが、前記ウのとおり、原告ら主張の注意義務を負わないので、被告ベネッセは、被告シンフォームを委託先として選任したことにつき注意義務を負わない。

10 また、被告ベネッセは、本件当時、平成21年経産省ガイドラインや情報セキュリティ対策の一般的な基準からしても、高度な水準で被告シンフォームに対する監督をしていた。そして、平成21年経産省ガイドラインは、委託先から委託契約に盛り込んだ個人情報管理に関する事項の遵守状況全般をチェックシート形式の書面等により定期的に報告を受け

15 けることを望ましい事項としているにとどまり、委託元が委託先が採用している個別のセキュリティ対策を調査・検討し、委託元が委託先の採用していない他の考えられるセキュリティ対策を講ずることを求めることは望ましい事項ともしていない。

15 したがって、被告ベネッセは、委託先選任監督義務を負うとはいえない。

オ 被告らの行為の違法性について

20 本件個人情報、社会生活を営む上で一定の範囲の他者に当然開示されることが予定されている個人の識別などのための単純な情報にとどまり、秘匿されるべき性質のものとはいえず、他人に知られたいと感ずる程度の低いものであって、プライバシーに係る情報として保護される程度は最も低い。本件漏えいによって想定される事態は、名簿業者から名簿を購入した事業者からの営業に係る商品や役務の取引を誘引するための広告宣

25 伝資料、パンフレットなどの送付、架電又はメールを受けることであり、これらは、種々雑多に送られてくる郵便物、通信の中に紛れ、目にし、耳にするものであり、それを他のものと区別することができるものでもなく、

また、欲しなければ捨て置く対応も容易に採り得る。そして、原告らは、本件漏えいにより財産的損害を被っておらず、今後、財産的損害を被る蓋然性や本件個人情報が悪用されるなどの蓋然性もない。

5 また、被告らは、自ら故意に本件漏えいをしたものではなく、本件個人情報  
5 情報がむやみに開示されないような措置を採っており、被告らによる侵害行為の態様としては悪質性がほぼ存在しない。

さらに、被告らは、本件漏えいを把握した後、速やかに謝罪し、事実調査をし、500円相当の補償を実施し、再発防止のために、相当の費用及び労力をかけて対策を講じた上、本件行為により甚大な被害を受けており、  
10 被告らにおいて本件行為につき賠償責任を負うとした場合には、企業としての存続の途を絶たれ、また、同種事件における悪影響も重大である。

したがって、被告らの本件漏えいに係る行為は、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。

#### カ 被告シンフォームのCを被用者とする使用者責任について

15 (ア) 本件行為の対象は、氏名、住所等の基本情報であるので、原告らに法的に賠償されるべき損害が生じたと評価ができないので、Cが原告らに対し本件行為につき不法行為責任を負うとはいえない。

(イ) また、システムの開発、運用、保守等を受託する企業の作業者が、委託元のシステムのアクセス権限を与えられ、同システムの開発等のために実際に同システムにアクセスすることは、システムの開発、運用、保守等を行う以上当然のことで、そのことから受託業務の遂行が委託元の事業の遂行であるかのような外観を当然に有するとはいえない。また、  
20 本件行為は、被告シンフォームの事業ではなく、Cの職務の範囲内にあるものでもないので、本件行為は、被告シンフォームの「事業の執行について」  
25 されたものに当たるとはいえない。

(ウ) 被告シンフォームの社員はCに対し日常的に指示をしていない上、被

告シンフォームによるCに対するアカウントの教示，本件パソコンの貸  
与及び研修の実施は使用関係がないことと矛盾せず，被告シンフォーム  
と委託先の会社との間では，契約上，業務遂行上の指示・管理その他指  
揮命令は全て委託先会社の指示命令者ないし責任者（以下「委託先責任  
5 者」という。）が行うものとされ，例外的に，緊急時やトラブル時に，  
被告シンフォームが委託先会社の要員に必要な範囲で直接依頼すること  
ができるとされており，実際も，委託先責任者がこれをしていた。

したがって，被告シンフォームは，Cを実質的に指揮監督する関係に  
あったとはいえない。

10 (エ) また，被告シンフォームは，Cから業務上知り得た個人情報及び機密  
情報を保秘する旨の同意書を受領しているほか，Cを含む業務従事者全  
員を対象に，毎年，情報セキュリティ研修及びその内容を踏まえたテス  
トを実施していたので，被告シンフォームは，Cとの関係に照らし，民  
法715条1項ただし書所定の「相当の注意をした」といえる。

15 (オ) よって，被告シンフォームは，原告らに対し，本件行為につきCを被  
用者とする使用者責任に基づく損害賠償責任を負うとはいえない。

キ 被告ベネッセの被告シンフォームを被用者とする使用者責任について

(ア) 被告シンフォームは，前記ウのとおり，本件行為に関して不法行為責  
任を負わない。

20 (イ) 本件業務が被告ベネッセの職務の範囲に属していることにつき，原告  
らの主張は失当である。

(ウ) 民法715条1項所定の「他人」は自然人を想定しており，法人を含  
まず，また，本件業務に関する被告ベネッセと被告シンフォームとの関  
係は，標準的なシステム開発契約における委託者と受託者との関係を超  
えるものではないため，被告ベネッセと被告シンフォームとの間に実質  
25 的な指揮監督関係はない。

(エ) また、被告ベネッセと被告シンフォームの関係は、基本的には業務委託という対等な取引関係であり、被告ベネッセは、被告シンフォームの選任及び監督に当たり、個人情報保護法上求められる義務を尽くしていたので、被告ベネッセは、民法715条1項ただし書所定の「相当の注意をした」といえる。

5

(オ) よって、被告ベネッセは、原告らに対し、本件行為につき被告シンフォームを被用者とする使用者責任に基づく損害賠償責任を負うとはいえない。

#### ク 原告らの損害について

原告らは、本件行為により、具体的損害、実質的損害を一切受けておらず、具体的損害・実質的損害が将来発生する蓋然性もなく、原告らが主張する損害は抽象的な不安感や不快感にすぎない。

10

本件個人情報、特に秘匿すべきプライバシーに関わる情報や主観的な価値に結びつく情報でなく、社会生活を営む上で開示を求められることが多い客観的な情報であるため秘匿性が低く、その開示相手や予想される利用形態等に照らして原告らの感じる不安感や不快感などの精神的負担も低い。また、被告らが自ら故意に本件個人情報を開示したのではなく、被告らに対する非難として損害を認める必要性もない。さらに、被告らは、情報漏えいの対象者に対して、「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」と題する書面（以下「本件通知書」という。）を送付し、500円相当の補償を提供し、相談窓口の設置等を行い、情報拡散防止活動なども継続的に行うなど事故後の適切な対応により原告らの精神的損害が慰謝されている。

15

20

なお、Cは、イベントで集めた情報として本件売却行為をしており、名簿業者に被告ベネッセに関連する情報である旨を伝えていないので、本件漏えいによって、子供の教育に熱心な、又は関心があるという属性は明ら

25

かになっていない。

したがって、原告らには、本件漏えいにより慰謝料を認める程の精神的損害が発生したとはいえない。

### 3 争点

- 5 (1) ①コード判明原告のうち、情報一覧表の認否欄の情報項目に「▲」、  
「△」又は「★」の記載がある情報、②コード帰属未定原告の情報、③コード不明原告の情報は、本件漏えい情報であるかどうか。
- (2) 被告らに、原告ら主張の注意義務違反の前提としての予見可能性があったかどうか。
- 10 (3) 被告シンフォームは、持込禁止義務、USB接続禁止義務、書き出し制御義務、アラート設定義務及び監視カメラ設置義務を負うかどうか。
- (4) 被告ベネッセは、部門設置義務、シンフォーム同様義務及び委託先選任監督義務を負うかどうか。
- (5) 被告らの行為が違法といえるかどうか。
- 15 (6) 被告シンフォームのCを使用者とする使用者責任があるかどうか。特に被告シンフォームとCとの間に指揮監督関係があるかどうか。
- (7) 被告ベネッセの被告シンフォームを被用者とする使用者責任があるかどうか。
- (8) 原告らの精神的損害の有無及び程度

### 20 第3 争点に対する判断

#### 1 本件漏えい情報（争点(1)）について

##### (1) コード判明原告について

- ア コード判明原告については、前提事実(7)のとおり、認否欄の情報項目に「○」の記載がある情報が漏えいしている。他方、コード判明原告につき、  
25 同情報項目に「★」の記載がある情報については、同情報が漏えいしたことについての証拠は全くない。

イ コード判明原告の認否欄の情報項目に「▲」の記載がある情報について

コード判明原告の認否欄の情報項目に「▲」の記載がある情報は、氏名、  
生年月日、郵便番号又は住所であり、また、被告らにおいて被告らが保有  
している情報の内容を主張するところ、証拠（甲65）によれば、被告ベ  
5 ネッセらは、顧客に手紙を送付し、又は電話をして、被告ベネッセその他  
の関連会社が実施する教育事業その他の事業に新規に、又は継続的に勧誘  
しており、そのために、被告らが原告らから取得した情報を管理していた  
ことが認められる上、被告らにおいて、原告らから取得した情報を変更し  
10 ていることをうかがわせる事情も見当たらないので、これらの事情からす  
れば、被告らが保有している情報が原告らから提供された情報であると推  
認するのが相当である。そして、まず、①氏名については、別紙原告目録  
の原告番号欄341の原告（以下、原告の特定については、同原告を「原  
告341」というなど同目録の原告番号を用いてする。）については、情  
報一覧表の認否欄の備考欄（以下「備考欄」という。）に「登録されてい  
15 た氏」と記載されている旧姓の氏が漏えいしたことは当事者間に争いがな  
い上、上記の理由により、被告らが保有していた情報は、備考欄に「登録  
されていた氏」又は「登録されていた名」と記載されている氏又は名であ  
るといえるので、原告114、176、181、182、1023、10  
24、1073から1075まで及び1116については、同氏又は名が  
20 漏えいしたといえることができる。また、②生年月日についても、同様に、  
被告らが保有していた情報は、備考欄に「登録されていた生年月日」と記  
載されている生年月日であるといえるので、原告44、80、135、2  
37及び1004については、同生年月日（ただし、具体的な日は特定す  
ることができない。）が漏えいしたといえることができる。③郵便番号及び  
25 住所についても、同様に、その住所について被告らが保有していた情報は、  
備考欄に「登録されていた住所」として記載された住所であるといえる

ころ、原告88、1001から1003まで、1007、1029、1067、1068、1118及び1119については、同住所及び原告88、1007、1118及び1119を除く同原告らにあってはこれに対応する郵便番号が漏えいしたとすることができる。

5           ウ   コード判明原告の認否欄の情報項目に「△」の記載がある情報について  
              コード判明原告の認否欄の情報項目に「△」の記載がある情報は、性別、  
              生年月日、住所、電話番号、ファクシミリ番号、メールアドレス、出産予  
              定日又は保護者の氏名であり、これらの情報自体の漏えいがあったことは  
              被告らも認めているものの、被告らにおいて、その内容については知らない  
10           としてしている。そして、このうち、住所については、原告らが虚偽の情報を  
              を提供する動機も見当たらない一方、被告らにおいても、上記イと同様に、  
              正確でない情報を保有する意味は見だし難いので、別紙原告目録の「漏  
              えい時住所」欄の住所が漏えいしたものと推認するのが相当である。他方、  
              生年月日については、前記イのとおり、戸籍上の生年月日とは異なるもの  
15           が含まれているのみならず、証拠（甲72）によれば、被告ベネッセらの  
              商品の送付を受ける時期を実際の生年月日の日より1年先又は1年後にす  
              るなどのために、不正確なものを提供していた者がいることが認められる  
              一方、原告らは、第25回口頭弁論期日において、その生年月日が戸籍上  
              のそれと同一であることを確認しておらず、また、性別、電話番号、ファ  
20           クシミリ番号、メールアドレス及び出産予定日については、具体的な内容を  
              を主張しないとし、また、保護者の氏名を特定しないので、正確でない情  
              報が含まれている可能性があるという限度で、これらの情報が漏えいした  
              と認めるのが相当である。

(2)   コード帰属未定原告について

25           弁論の全趣旨によれば、コード帰属未定原告は、被告ベネッセから送付さ  
              れた本件通知書に記載されていた登録コードがあった一方、被告らにおいて

登録コードがコード帰属未定原告に係るものであることを確認することができないのは、被告ベネッセが、本件通知書の発送後、原告ら等からの要請を受けて、登録コードに係る個人情報を抹消しているためであると認められるところ、これらの事実に加え、同原告の主張する登録コードが同原告のもの  
5 ではないことをうかがわせる事情がないことに照らせば、コード帰属未定原告の登録コードは、当該原告の登録コードであると推認することができる。

そして、コード帰属未定原告の情報一覧表の認否欄の情報項目に「▲」又は「△」の記載がある情報について、上記原告らの情報の漏えいがあったことについては被告らも認めているところ、前記(1)イ及びウのとおり、同認否  
10 欄の氏名に「▲」の記載があるものについては、備考欄に「登録されていた氏」又は「登録されていた名」と記載されている氏又は名が漏えいされ、また、同「△」の記載がある情報については、その情報の内容に正確でないものが含まれている可能性があるという限度で漏えいがあったと認めることができる（なお、原告69から73までについては、同認否欄の情報項目に  
15 「△」の記載がある情報が、氏名、性別、生年月日、郵便番号、住所及び電話番号のほか、3名につき保護者の氏名、残りの1名につきメールアドレスであるところ、弁論の全趣旨によれば、原告69が原告70から73までの保護者であると認められるので、氏名、性別、生年月日、郵便番号、住所及び電話番号のほか、原告70から73までにおいて保護者の氏名が、原告6  
20 9においてメールアドレスが漏えいしたと認めるのが相当である。）。他方、同認否欄の情報項目に「★」の記載がある情報については、同情報が漏えいしたことについての証拠は全くない。

### (3) コード不明原告について

ア 原告3は原告5の、原告18及び19は原告20の、原告22は原告2  
25 4の、原告26は原告28の、原告29は原告30及び31の、原告32は原告34の、原告47は原告49及び50の、原告60は原告62の、原告

74は原告75の、原告123は原告125の（ただし、保護者の氏名は「D」）、原告127は原告129の、原告137は原告138の、原告179は原告181及び原告182の（ただし、保護者の氏名は「F」）、原告180は原告182の（ただし、保護者の氏名は「G」）、原告202は原告204の、原告211は原告212の、原告240は原告242の、原告253は原告255及び256の、原告303は原告304の、原告352は原告353の、原告1084は原告1086の、原告1087は原告1088の、原告1101は原告1102のそれぞれ保護者として登録されていた者の氏名と一致する者であり、登録されていた保護者の氏名が漏えいしたことは当事者間に争いがないので、いずれもそれぞれ原告3, 18, 19, 22, 26, 29, 32, 47, 60, 74, 123, 127, 137, 179, 180, 202, 211, 240, 253, 303, 352, 1084, 1087及び1101（以下「保護者原告」という。）においては、その被保護者である未成年原告らの保護者として、その氏名が漏えいしたものと認めることができる。そして、保護者原告については、証拠（甲14の1から3まで、B32の1, 2, B119の1, B219の1）によれば、未成年原告を情報漏えいの対象者とする本件通知書はその保護者である成年原告に宛てて送付していることや、登録者の情報につき、本件通知書には「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を記載していることが認められ、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、保護者原告の氏名が漏えいされていれば、氏名のほか、保護者原告の被保護者である未成年原告らと同じ情報（保護者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限る。）も保護者原告の情報として漏えいしたと見るのが相当である。

イ 原告48, 57, 92, 93, 104, 145, 146, 218から2

20まで、314、315、358、359、1113及び1114については、証拠（甲B48の1、B57の1、B92の1、2、B104の1、B145の1から5まで、B219の1、B220の1、B314の1、2、B358の1、B1113の1、2、B1114の1）及び弁論の全趣旨によれば、これらの原告らは、被告ベネッセから、同原告らを情報漏えいの対象者とする本件通知書を受領し、同原告らの多くにおいて謝罪の品としての全国共通図書カード500円分又は電子マネーギフト500円分（以下「本件謝罪品」という。）を受領していることが認められる。これらの事実に加え、本件通知書に情報漏えいの対象者として記載された者は、個人情報

5  
10  
15  
20  
25

の漏えいがあったことを被告ベネッセにおいて確認することができた者であること（弁論の全趣旨）に照らすと、同原告らの個人情報が本件行為により漏えいしたと推認することができる。

そして、上記各原告の漏えいした個人情報の内容について、証拠（甲1、14の1から6まで、甲53の1、乙3の1、乙30）によれば、被告ベネッセらが平成26年7月9日に公表した「お客様情報の漏えいについてお詫びとご説明」と題する書面には、漏えいが確認されている情報項目として、郵便番号、顧客（子及びその保護者）の氏名、住所、電話番号、子の生年月日、性別が記載され、また、本件通知書、被告ベネッセらが同年9月10日に公表した「お客様情報の漏えいに関するご報告と対応について」と題する書面及び平成29年8月頃に作成した「事故の概要」と題する書面には、漏えいが確認されている情報として、①「サービス登録者」の氏名、性別及び生年月日のほか、②同時に登録していた保護者又は子の氏名、性別、生年月日及び続柄があり、その他に、③郵便番号、④住所、⑤電話番号、⑥登録している者のみにつきファクシミリ番号並びに⑦一部のサービスの利用者につき出産予定日及びメールアドレスが含まれている旨の記載があり、経産省が平成26年8月に公表した文書にも漏えい内容

として、氏名、住所、電話番号、子の生年月日、性別、一部のみにつき出  
産予定日とメールアドレスが含まれていると記載していることが認められ  
るところ、これらの事実のとおり、被告ベネッセらにおいては、公表等を  
した漏えいが確認されている情報につき、ファクシミリ番号、メールアド  
5 レス及び出産予定日には顧客の一部に係るものなどの留保を付している一  
方で、氏名、住所、電話番号などにはそのような留保を付していないのみ  
ならず、被告ベネッセらは、前記(1)イのとおり、顧客に手紙を送付し、電  
話をするために、本件個人情報を保管していたことからして、少なくとも、  
氏名のほか、これらの連絡のために必要な郵便番号及び住所又は電話番号  
10 を保有していたと見るのが自然であり、さらに、前提事実(7)並びに前記(1)  
イ及びウのとおり、コード判明原告の全部について、氏名のほか、郵便番  
号及び住所又は電話番号が漏えいしていることに照らすと、原告48、5  
7、92、93、104、145、146、218から220まで、31  
4、315、358、359、1113及び1114についても、少なく  
15 とも、それぞれ氏名のほか、郵便番号及び住所又は電話番号が漏えいした  
(ただし、氏名については、同イのとおり、戸籍上の氏名でないものが同  
原告らから提供された情報であることがあるところ、通称などのほか、証  
拠(甲68、72)によれば、被告ベネッセらの顧客には、被告ベネッセ  
らにあえて戸籍上のものと異なる氏名を提供していた者もいると認められ  
20 ることからすると、戸籍上のものでないものが含まれている可能性がある  
という限度で認められ、また、同ウのとおり、電話番号についても、正確  
でない情報が含まれている可能性があるという限度で認められるにとどま  
る。)と認めるのが相当である。

ウ 一方、原告6及び58の個人情報が漏えいしたことについては、証拠が  
25 全くない。

エ また、原告7については、証拠(甲B7の1)によれば、被告ベネッセ

は、原告7に対し、「H」を情報漏えいの対象者とする本件通知書を送付していることが認められるものの、原告7と「H」とは、氏を共通にするものの、両者の関係を明らかにする証拠はないので、原告7の個人情報が漏えいしたとは認められない。

5           さらに、原告119、297及び351については、証拠（甲B119の1から4まで、B297の1、2、B351の1）によれば、被告ベネッセは、原告119に宛てて、原告120を情報漏えいの対象者として、本件謝罪品を交付し、また、原告297又は原告351に宛てて、原告298及び原告299又は原告354を情報漏えいの対象者として、本件通知書を送付していることが認められるけれども、被告らにおいて、原告120の保護者として原告119の氏名が、原告298及び299の保護者として原告297の氏名が、原告354の保護者として原告351の氏名が、それぞれ登録されていたことを確認することができないと主張しているのみならず、原告119、297、351を情報漏えいの対象者とする本件通知書が送付されていることを裏付ける証拠がなく、また、被保護者を対象者として送付する本件通知書や本件謝罪品在中の封書の名宛人だけを保護者である同原告らとしていた可能性を払拭することができる事情も見当たらないので、これらの事実からだけでは、原告120の保護者として原告119の氏名、原告298及び299の保護者として原告297の氏名、原告354の保護者として原告351の氏名が登録されていたと認めるには足りない。そうすると、原告119、297及び351の個人情報が漏えいしたとは認められない。

10  
15  
20  
25           (4) 以上によれば、本件行為により、原告6、7、58、119、297及び351の6名については、個人情報が漏えいしたとは認められないけれども、その余の原告（別紙原告目録の判断欄に○と記載した原告ら）については、情報一覧表の各原告に対応する項の認定欄の情報項目欄に「○」及び「●」の記載がある情報（ただし、「●」の記載がある情報にあつて郵便番号及び

住所又は電話番号のいずれかの情報，原告69から73までにあつて前記(2)のとおり)が漏えいしたと認められる一方，同情報項目欄に「×」の記載がある情報は漏えいしたと認めることはできない。

## 2 被告らの予見可能性（争点(2)）について

### 5 (1) 認定事実

括弧内の証拠等によれば，以下の事実が認められる。

ア 平成21年経産省ガイドラインは，個人情報保護法8条に基づき個人情報保護法に定める事項に関して必要な事項を定め，経産省が所管する分野及び個人情報保護法36条1項により経済産業大臣が主務大臣に指定された特定の分野における事業者等が行う個人情報の適正な取扱いの確保に関する活動を支援する具体的な指針として定めることなどを目的としている。平成21年経産省ガイドラインは，経済産業大臣が個人情報保護法を執行する際の基準となるものであり，「しなければならない」と記載されている規定については，それに従わなかった場合には，経済産業大臣によって，  
10 個人情報保護法の規定違反と判断され得る一方，「望ましい」と記載されている規定についても，それに従わなかった場合でも，個人情報保護法の規定に違反することはないものの，個人情報保護法の基本理念を踏まえ，個人情報保護の促進の観点から，できるだけ取り組むことが望まれるものとされている。

平成21年経産省ガイドラインには，安全管理措置（個人情報保護法20条関連）という項目において，個人情報取扱事業者がその取り扱う個人データの漏えい，滅失，き損の防止その他の個人データの安全管理のため，組織的，人的，物理的及び技術的な安全管理措置を講じなければならず，その際，本人の個人データが漏えい，滅失又はき損等をした場合に本人が  
20 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，必要かつ適切な措置を講じるものとし，  
25

その際には、個人データを記録した媒体の性質に応じた安全管理措置を講  
じることが望ましいとの記載の後に、組織的安全管理措置のうち、個人デ  
ータの取扱いに関する規程等に記載することが「望まれる」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。）」との記載がされて  
いる。

5  
10  
15  
20  
なお、平成21年経産省ガイドラインは、平成26年12月12日に、  
同年厚生労働省・経産省告示4号により改訂された。同改訂では、組織的  
安全管理措置に関して、個人データの取扱いに関する規程等に記載するこ  
とが「望ましい」事項の例として、「個人データを閲覧だけできる端末」  
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  
ることに加え、「スマートフォン、パソコン等の記録機能を有する機器の  
接続を制限し、媒体及び機器の更新に対応する」旨が追記され、また、物  
理的安全管理措置に関して、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、「入退館（室）の際における業務上許可を得て  
いない記録機能を持つ媒体及び機器の持ち込み及び持ち出しの禁止と検査  
の実施」と「カメラによる撮影や作業への立ち会い等による記録又はモニ  
タリングの実施」が追記されている。

(甲7, 乙10, 12)

20  
イ 独立行政法人情報処理推進機構は経産省所管の独立行政法人であるところ、平成25年IPAガイドラインは、違法行為だけでなく、情報セキュリティに関する内部規程違反等の違法とまではいえない不正行為をも内部不正に含めて、組織内における具体的な内部不正対策を検討している。そ  
25  
して、平成25年IPAガイドラインでは、個人の情報機器及び記録媒体の業務利用及び持込みの制限として、「個人のノートPC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を制限しなければならない」とした上で、リスクとして、個人の情報機器及び記録媒体を業務に利用すると、個人の情報機器及び記録媒体の組織による管理が困難であることや、個人と組織の情報が共に扱われることから、ウイルス感染や操作ミス等によって重要情報が漏えいする可能性が高くなるとし、「重要情報を取り扱う業務フロア等の領域に個人の情報機器及び記録媒体を持ち込まれると、個人の情報機器や記録媒体に重要情報を格納して持ち出される恐れがあ」と指摘して、対策のポイントとして、個人の情報機器及び記録媒体の業務利用及び持込みの制限では、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とした上で、具体的な対策として「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込み・利用を厳しく制限」し、また、「個人所有のUSBメモリ等の携帯可能な記録媒体等の持込みを制限」することを定めて運用すると記載されている。

(甲9, 乙15の1, 弁論の全趣旨)

ウ JIS基準は、事業者が、その取り扱う個人情報のリスクに応じて、漏えい、滅失又はき損の防止その他の個人情報の安全のために必要、かつ適切な措置を講ずることを求めているところ、これを受けて、平成22年JISガイドラインは、事業者において、リスクなどの認識、分析及び対策に基づき、個人情報のライフサイクルの観点から決定することとなる対策の例示として、取得・入力局面及び利用・加工局面で、個人情報を入力し、又は利用・加工することが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の例示として、個人情報を入力することができる端末や個人情報を閲覧だけすることができる端末では、CD-ROM, USBメ

メモリ等の外部記録媒体を接続することができないようにすることが挙げられている。

(甲22)

エ 日本データセンター協会は、データセンター事業者と、データセンター事業者を取り巻く関連事業者との協力体制を構築し、データセンターへの社会的要請に協力して当ることによってデータセンター事業の強化・発展をさせることを目的とする特定非営利活動法人である。平成25年データセンターガイドブックは、データセンターのエントランス区画では、データセンター事業者から許可された機器や荷物以外を持ち込ませないことにより、館内、特にサーバーに悪影響を与えるおそれのある対象物を排除することを目的として、USBメモリ等の情報記録媒体を持ち込みが制限される品目の1つとして挙げ、また、サーバー室では、情報の不正持ち出しの脅威に対し、記録媒体の持ち込みを禁止するルールを管理策として挙げている。

15 (甲20, 弁論の全趣旨)

オ 被告シンフォームは、平成23年7、8月に、業務用パソコンに搭載した本件セキュリティソフトをバージョンアップし、全てのデバイスを制御することができる機能を有していたものの、本件当時、「リムーバブル、CD/DVD、外付けHDD」の書き出しの制限のみを設定していたため、MSCによるデータ通信に対し書き出しを制御することができるのにとどまっていた。なお、被告シンフォームは、本件当時、業務上の必要性が明確で、他の方法がなく、情報の部門責任者及び各部管理責任者の外部メディアの使用許可を得た場合でない限り、その制御を解除しない扱いをしていた。

25 また、被告シンフォームは、業務用パソコンと本件データベースを含まない連携システムのデータベースサーバとの間の通信量が一定の基準値を

超えた場合、連携システムのデータベースの管理者である被告シンフォームの各担当部門の部長に対して、メールでアラートが送信される仕組みを採用していた。

(甲2, 12の1, 2, 甲19の3, 甲65, 69から71まで)

5 カ アンドロイド4.0が平成23年10月18日にリリースされたところ、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の平成24年夏発売のアンドロイドスマートフォンの多くはアンドロイド4.0であった。

10 また、株式会社MM総研は、平成25年3月28日、同年1月末のスマートフォン契約数が4061万件となり、そのうちアンドロイドスマートフォンが2570万件(63.3%)、iOSをOSとするスマートフォン(以下「アイフォン」という。)が1412万件(34.8%)、それ以外のOSが79万件(1.9%)であって、アンドロイドスマートフォンのシェアが平成23年3月の40.4%から22.9ポイント増加する一方、アイフォンは同月の49.6%から14.8ポイント減少していると指摘している。

20 そして、日本写真印刷コミュニケーションズ株式会社は、平成25年8月2日、アンドロイドスマートフォンのOSのバージョンシェアについて、同年4月時点において、アンドロイドスマートフォンの契約数のうち、半数を超えるものがアンドロイド4.0以降のバージョンものであることを公表している。なお、同シェアについては、世界全体のものを指しているとの指摘がある。

(甲40, 41, 51の1から3まで, 乙97)

25 キ 他方、株式会社インターネットプライバシー研究所は、平成29年3月15日作成の意見書の中で、携帯電話端末の全体のうちのスマートフォンの割合が平成24年3月末時点で22%、平成25年3月末時点で36%、

平成26年3月末で48%となるどころ、そのうち、アンドロイド4.0は、平成24年6月時点で0.15%未満、平成25年6月時点で7.16%、平成26年6月時点で10.28%であることを指摘するほか、携帯電話端末の契約数が、平成24年3月末時点で1億件を超えて、平成25年3月末には更に増加し、平成26年3月には1億2万件を超えて、平成26年12月末には1億2511万件となったことを示す資料を添付している。

また、平成24年10月から12月にかけて実施された調査において、スマートフォンの販売シェアのうちアンドロイドスマートフォンは31.9%であった旨を指摘する平成25年1月のインターネット記事や、平成24年、平成25年、平成26年のアンドロイドスマートフォンのスマートフォン全体に占めるシェアがそれぞれ25%、41.9%、39.6%とするインターネットの記事がある。

(乙34, 70, 71)

ク 日経コンピュータの記者は、平成26年7月30日、「ベネッセ事件容疑者はなぜスマホでデータを持ち出せたか、IT部門は設定の再点検を」と題する記事を公表している。同記者は、同記事の中で、MTPの存在が情報漏えい対策の盲点になり得ること、アンドロイドスマートフォンの場合、本格的には遅くとも平成23年10月公開のバージョン4.0からMTPによるファイル転送に対応していること、商用デバイス用のセキュリティソフトでは、一般にUSBマストレージの使用制限に加え、ウインドウズ・ポータブルデバイスの使用を制限することでスマートフォンのデータ転送を制限することができること、同セキュリティソフトがMTPやウインドウズ・ポータブルデバイスの使用制御機能に対応した時期は、日本電気株式会社製のものが平成19年7月、株式会社日立ソリューションズ製のものが平成21年6月、エムオーテックス株式会社製のものが平成

23年3月、日本ファインアート株式会社製のものが平成23年8月、ハミングヘッズ株式会社製のものが平成23年12月、株式会社インテリジェントウェイブ製のものが平成24年7月、富士通株式会社製のものが平成25年8月であることを記載するとともに、マイクロソフト製品のセキュリティに詳しいIによる「この穴」は平成25年頃からセキュリティ技術者の間で話題となっていたとの指摘を紹介した上で、バージョン4.0まではMTP対応端末が少なく、現実的な脅威でなく、被告ら以外の企業のIT部門でも、「USBメモリーは制御しても、MTPの設定までは思い至らない例は多いのでは」との同人のコメントを紹介するなどしている。

10           なお、商用デバイス用のセキュリティソフトの平成26年6月当時の国内市場シェアにつき、日本電気株式会社製のものが4.1%、株式会社日立ソリューションズ製のものが17.8%、エムオーテックス株式会社製のものが18.8%、日本ファインアート株式会社製のもの及びハミングヘッズ株式会社製のものが不明で、株式会社インテリジェントウェイブ製のものが0.4%、富士通株式会社製のもの2.4%との報告がある。

(甲16, 乙35)

ケ 株式会社インターネットプライバシー研究所は、平成29年3月15日、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調査を行ったところ、実用的なMSC制御機能は全ての製品に搭載されていた一方、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製品にとどまっており、しかも、その製品の初期設定もMTP制御機能は無効とされている旨を報告している。ここでいう「実用的」の意味は、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

不可能とする設定をいう。)ができる場合としている。そして、同研究所は、平成30年9月20日、一般の企業等の業務において、デジタルカメラ、デジタルビデオカメラ、ボイスレコーダーの画像・動画・音声の情報をMTP通信によりパソコンに取り込むことは日常的に行われているとの認識を示した上で、MTP通信による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た意見書を作成している。

(乙35, 96)

コ 株式会社エネルギー・コミュニケーションズのIは、平成28年2月5日に「情報セキュリティの運用面での脆弱性情報にも届出制が必要なのではないか」という論考をウェブページに掲載した。同人は、同論考の中で、平成24年には、アンドロイド4.0以降では、ファイル転送にMTPが採用されており、情報漏えいに悪用できるのではないかと気付いたところ、当時、この問題に気付いて警笛を鳴らす者や、国の機関・組織もないものの、セキュリティ対策が新たに生まれたリスクに対応していないことを考慮して、公表をしなかった旨記載している。

(乙36)

サ 工学院大学名誉教授Jは、平成30年1月15日、被告ベネッセから依頼を受けて、意見書を作成した。同人は、その意見書の中で、平成26年当時、MTPを利用した情報漏えいの危険は知られていなかった旨の認識を明らかにしている。

また、株式会社インターネットプライバシー研究所は、平成29年1月23日及び平成30年9月20日に作成した意見書の中で、本件当時、MTP通信を利用することができるスマートフォンの情報漏えいリスクは、情報セキュリティの専門家でも、ほとんど認識されていなかったと指摘している。

(乙24, 91, 96)

シ 日本ネットワークセキュリティ協会理事等を務めるKは、平成29年3月30日、MTPに対応しているウインドウズ・パソコンに、アンドロイド4.0を接続し、パソコンのドキュメント情報をスマートフォンに書き出した場合でも、スマートフォンではパソコンのドキュメント情報を閲覧  
5 することができないと指摘している。

(乙32)

(2) Cは、前提事実(5)のとおり、本件パソコンのUSBポートにUSBケーブルを用いてMTP対応のスマートフォンを接続し、MTP通信によりデータを転送する方法によって、本件取得行為をしているところ、MTP通信は、  
10 前提事実(6)のとおり、従来から多く利用されているMSCによるデータ通信とはその通信方法を全く異にする（なお、前記(1)認定事実オ及びクのとおり、MTP通信とMSCによるデータ通信とはその制御方法も異にするところ、被告シンフォームでは、本件当時、業務用パソコンにおいて、MSCによるデータ通信に対しては書き出しを制御する措置を施していた。）ので、被告  
15 らが本件行為に関し原告らの主張の注意義務を負うとするには、その前提として、被告らにおいて、本件当時、パソコンのUSBポートにUSBケーブルを用いてMTP対応の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個人情報を不正に取得されることを予見し得たことを要すると解される。

(3) そして、まず、前記(1)認定事実アからエまでのとおり、本件行為の前から、平成21年経産省ガイドラインや平成25年IPAガイドライン等では、個人データを入力することができる端末には外部記録媒体を接続することを禁止する方法を推奨し、また、重要情報を取り扱う業務フロア等において、個人の情報機器や外部記録媒体に重要情報を格納して持ち出される危険性に鑑  
25 み、スマートフォン等のモバイル機器等及び外部記録媒体の持込みを制限すべきである旨指摘するなどしているところ、これらは行政機関その他の団体

による個人情報を取り扱う事業者等に対する一定の指摘事項であるため、被告らにおいては、本件当時、スマートフォン等の情報機器を利用した情報漏えいがあり得ることを想定することができたといえる。また、被告らにおいても、実際、同認定事実オのとおり、被告シンフォームが、本件当時、外部メディアへの書き出し制御措置を採っていたから、被告らも、外部記録媒体一般については、パソコンのUSBポートに接続して、個人情報を不正に取得される可能性を認識していたと認められる。

また、前記(1)認定事実カ及びキのとおり、平成24年夏発売の 안드로이드スマートフォンの多くがMTPに対応している 안드로이드4.0であり、平成25年には 안드로이드4.0が我が国国内において少なくとも数百万件を超える相当多数販売されていたといえる。また、同認定事実クのとおり、MTPに対応した商用デバイス用のセキュリティソフトが平成19年から販売されて、平成26年当時には広く利用されていたこと、証拠(甲97)によれば、株式会社C&Cアソシエイツ製のセキュリティソフトの説明には、平成24年3月頃、WPD制御機能につき、スマートフォン等のWPD機器を制御することで更なる情報漏えい対策を強化することができることを記載しているものがあると認められることを考慮すると、本件当時、MTP通信を利用したスマートフォンへの情報の書き出しについても、被告らは予見することができたとみる余地があるとも思える。

しかしながら、MTPは、前提事実(6)のとおり、元来、音楽・映像ファイルを送送するための規格であって、MTP通信によるドキュメントファイルの送送が可能であることを説明する取扱説明書等の文書等があることを裏付ける証拠がないので、 안드로이드4.0が多数販売されていたからといって、本件当時、MTP通信によりドキュメントファイルを送送して不正に情報を取得することが一般に認識される状況となっていたとはいえず、また、MTP接続制御機能を備えたセキュリティソフトも、音楽・映像ファイルの

転送をさせる必要性がない場合に機能させることを想定して設けられたと見る余地もあり、上記のとおり、同セキュリティソフトが広く出回っていることから、MTP通信を利用したスマートフォンへの情報書き出しの危険性を認識し得たとするのは困難である（なお、証拠（甲96の1）によれば、本件セキュリティソフトについて、情報漏えい対策に関する記載がないまま、スマートフォンへの出力を制御することができる効果のみを説明している記事があることが認められる一方、上記のような情報漏えいの危険性の防止の観点からWPD制御機能を説明しているセキュリティソフトは、被告シンフォームが業務用パソコンに導入したものとは異なる（甲97）上、同様の説明をしているものが一定程度広くあることをうかがわせる証拠がないことに照らすと、そのような説明がされることが一例あっただけで、被告らにおいて、ドキュメントファイルのMTP対応のスマートフォンへの書き出しを予測することが可能であったと見るべき事情としては足りない。）。そして、MTP通信を利用したスマートフォンへの不正な情報書き出しの事例が本件行為の前になかった（弁論の全趣旨）のみならず、前記(1)認定事実ク、コ及びサのとおり、MTP通信を利用した不正な情報書き出しの危険性につき、平成24年には認識していたとする者や、平成25年頃からセキュリティ技術者の間で話題となっていたとの指摘はあるものの、これらは公表されてはおらず、他方、専門家の中にも、上記危険性を認識していた者がいなかったと指摘する者もいる上、同認定事実コに加え、証拠（乙32）及び弁論の全趣旨によれば、本件当時において、MTP通信を利用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指摘した行政機関その他の団体の基準等がないことが認められる（なお、原告らは、MTP通信に限定した情報書き出しの危険性について本件当時までに公表した文献（枝番号を含む甲101から104まで、106）等が新たに発見されたなどとして、口頭弁論の再開を求めるけれども、本件当時までに公表されたセキュリティソフトの商品説

明において、MTPに対応した外部メディア制御機能に関しUSB接続を介した企業データ情報漏えい対策の強化を指摘する例（甲101の1，2）があったとしても、この例が上記例に加わることにより上記の事情の判断を左右するものとはいえず、また、別のセキュリティソフトの商品説明において、  
5 本件行為と酷似する例を紹介した上で、「MTPデバイス問題」として、スマートフォンがMTPデバイスとして動作するために書き込みができる問題があることを指摘するもの（甲103の2）は、本件当時までに公表されたものではなく、その他の証拠も本件の判断に影響を及ぼすものではないので、口頭弁論の再開をする必要は見いだせない。）。

10 以上のような、行政機関その他の団体による個人情報の取扱いに関する指摘事項の内容や、MTP対応のスマートフォン及びセキュリティソフトの普及状況を踏まえても、MTPの基本的な用途等に加え、本件行為の前にMTP通信を利用したスマートフォンへの情報書き出しの事例がないこと、本件  
15 当時前における同情報書き出しの危険性に関する専門家の認識の状況、その危険性に関する指摘の公表及び行政機関その他の団体の基準等の不存在の状況などを総合考慮すると、個人情報を取り扱う企業又は個人情報を対象としたシステムの開発等をする企業である被告らにおいて、本件当時において、  
20 スマートフォンをパソコンのUSBポートに接続して個人情報を不正に取得される可能性を予見する可能性があるといえても、MTP対応のスマートフォンをパソコンのUSBポートに接続することによりMTP通信を利用して個人情報を不正に取得されることを予見する可能性があったとまでは認められない。

したがって、被告らは、本件当時、業務用パソコンのUSBポートにUSB  
25 Bケーブルを用いてMTP対応の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個人情報を不正に取得することの予見可能性があったということとはできない。

### 3 被告シンフォームの注意義務（争点(3)）について

前記2のとおり，原告らの主張する被告シンフォームの注意義務があるというためには，被告シンフォームにおいて，本件当時，パソコンのUSBポートにUSBケーブルを用いてMTP対応の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個人情報をも不正に取得されることを予見し得たことが前提となるところ，この予見可能性があったといえない以上，その余の点を検討するまでもなく，被告シンフォームは，持込禁止義務，USB接続禁止義務，書き出し制御義務，アラート設定義務及び監視カメラ設置義務のいずれも負うということとはできない。

10 なお，原告らは，被告シンフォームには，更にアクセスログ・通信ログの記録やモニタリングを行い，かつ，事業場に周知する義務及びアクセス権限を適切に管理する義務があった旨の主張もするけれども，これらの義務があるといえるためにも，上記の予見可能性があったことが前提となるといえるところ，同予見可能性があったといえない以上，これらの義務があったともいえないので，原告らのこの主張も採用することはできない。

### 4 被告ベネッセの注意義務（争点(4)）について

前記2のとおり，原告らの主張する被告ベネッセの注意義務があるというためには，被告ベネッセにおいて，本件当時，パソコンのUSBポートにUSBケーブルを用いてMTP対応のスマートフォンを接続しMTP通信によりデータを転送する方法によって個人情報をも不正に取得されることを予見し得たことが前提となるところ，この予見可能性があったとはいえないので，被告ベネッセは，その余の点を検討するまでもなく，部門設置義務を負うとはいえない。

また，同様の理由に加え，前記3のとおり，被告シンフォームに原告ら主張の注意義務がない以上，その注意義務があることを前提とする被告ベネッセの原告ら主張の注意義務もあるとはいえないので，その余の点を検討するまでもなく，被告ベネッセは，シンフォーム同様義務及び委託先選任監督義務を負う

ということとはできない。

5 被告らの過失による不法行為責任及び被告ベネッセの使用者責任について

5 以上によれば、被告らの過失による不法行為は、その余の争点（争点(5)及び(8)）について判断するまでもなく、認められず、被告ベネッセの被告シンフォームを被用者とする使用者責任も、被告シンフォームの不法行為が認められない以上、その余の争点（争点(7)及び(8)）につき判断するまでもなく認められない。

6 被告シンフォームの使用者責任の有無（争点(6)）について

(1) 認定事実

10 証拠（甲2、12の1、2、甲19の3、甲63、64、66、73）によれば、以下の事実が認められる。

ア 被告シンフォームでは、事業開発本部の下にある事業開発部に、本件システムに関する開発、運用、保守等を所管する課として顧客分析課を置いていた。顧客分析課は、多摩事務所において、本件業務のほか、顧客である被告ベネッセのために、本件システムを使用したデータの集計業務（被告ベネッセから特定の条件による契約者のリストの要望を受けてその契約を  
15 している人のリストを収める業務をいう。以下同じ。）や、QA対応業務（被告ベネッセからの本件システムの使い方等の問合せに対する回答をする業務をいう。以下同じ。）をしていた。被告シンフォームは、委託先との間で、業務委託個別契約を締結し、本件業務の一部を委託しており、その委託先、更にその委託先の委託先がその一部を再委託又は再々委託をするなどもしており、顧客分析課には、平成26年4月当時、39名が所属していたものの、そのうち、被告シンフォームの社員が11名で、その余の28名が複数の委託先（その委託先等を含む。）の従業員であった。

25 なお、本件システムは、平成24年4月から開発が開始され、平成25年4月に一部利用が開始し、運用開始予定としていた平成26年4月に一

応の完成を経た後も、本件当時まで、開発が続けられていた。

イ 顧客分析課の中には、チームが存在し、チームの中には個別案件を進めるために、更にメンバーなどと呼ばれるグループが存在していた。すなわち、顧客分析課において、個別案件の依頼を受けると、被告シンフォームの社員がその個別案件を処理するグループのリーダーとして決定され、同  
5 リーダー（以下「グループリーダー」という。）においてグループに属する人を選定して、グループを編成する。その後、グループリーダーは、作業ごとの計画を定め、スケジュールを管理し、案件の処理を進めていく。作業の進捗状況については、グループ内で、毎日又は毎週、進捗会議と呼ば  
10 ばれる打合せをし、前日の作業状況や当日の予定等を話し合い、共有していた。また、グループリーダーは、作業の遅れが生じた場合には、作業に余裕がある別のグループに属する人を探し、同人に作業を依頼するなどしていた。

ウ Cは、被告シンフォームの委託先の再々委託先の従業員であり、被告シン  
15 フォームから、業務に従事する前に、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、同テストに合格した。また、Cは、被告シンフォームから、その後も、平成24年から平成26年までの間、年1回実施される情報セキュリティ研修を受けていた。

エ Cは、顧客分析課で開発チームに所属した上で、複数のグループに属し、  
20 本件システムの開発作業に従事していた。

Cは、グループリーダーから、平成24年6月頃からは、業務の具体的な指示を直接受けて、それに応じていた上、作業の途中で問題が生じた場合には、グループリーダーに相談していた。また、Cは、グループリーダーから、1日で終わらない作業を割り振られることがあったほか、終業時間  
25 間の際に作業を依頼され、又は終業時間後の時刻に設定される打合せに出るよう依頼を受けるなどの残業の指示を受け、それに応じていた。さら

に、Cは、多摩事務所に出勤することができない事情がある場合には、グループリーダーに相談するなどしていた。

オ Cは、本件システムの開発作業のほか、QA対応業務をしていた。すなわち、QA対応業務においては、被告ベネッセの社員が、グループリーダー又はCに対し、本件システムの利用に関して、メールでの問合せをし、  
5 グループリーダーからCに対し同メールに回答をしておくようにというメールを受け、Cは、被告ベネッセの社員に対し、質問に対する回答を行っていた。そのようなやり取りを続けているうちに、Cは、被告ベネッセの社員から直接メールや電話での問合せを受け、被告ベネッセの社員に対し、  
10 直接回答するということがあった。

また、Cは、グループリーダーから依頼されて、委託先において受託していない集計業務もすることもあった。

さらに、Cは、グループリーダーから依頼を受けて、被告ベネッセからのデータの調査依頼がある場合にそれに対する回答が直ぐにできるように  
15 するため、被告シンフォームが被告ベネッセに対して作業の進捗を報告するために週1回実施している会議に出席することがあった。

カ Cは、委託先に労働時間を報告するほか、被告シンフォームに対しても、残業を含む労働時間について、業務日報又は管理表と呼ばれるシステムに、  
20 毎日の作業時間を入力して報告し、被告シンフォームにおいて管理されていた。

(2)ア 被告シンフォームは、前記(1)認定事実ウのとおり、Cとの間で雇用関係がないものの、Cに対し、情報セキュリティ研修等を受講させていただ  
25 けでなく、同認定事実イ及びエからカまでのとおり、本件システムの開発等の作業において、被告シンフォームの社員において、案件ごとに組成されたグループに属するように指示し、そのグループリーダーである被告シンフォームの社員において、具体的な仕事を割り振り、スケジュールを管理

し、日常的に直接指示をしていたほか、残業の指示をし、それらの指示に応じて業務に従事させ、また、労働時間の報告を受けるなど労務管理をしていたといえることができる。

イ これに対し、被告シンフォームは、委託先の会社との間では、契約上、  
5 委託先の従業員に対する業務遂行上の指示又は管理その他指揮命令は全て委託先責任者が行うとされており、グループリーダーが当該案件で委託する範囲について委託先責任者に対し具体的な業務指示を依頼し、委託先責任者において委託先の従業員に対し業務指示を行う仕組みが採られ、それが実態であったと主張し、刑事公判廷において、顧客分析課課長Lは、  
10 グループリーダーが委託先の従業員に対し直接指示をすることは原則ない旨供述し（甲66〔46ページから49ページまで〕）、事業開発本部長兼事業開発部長Mも、委託先の従業員については、緊急性の高い場合等を除き、委託先責任者を通じて、業務の指示をすることとなっており、委託先責任者が委託先の従業員の残業を指示していた旨供述する（甲73〔33  
15 ページから37ページまで、58ページから60ページまで、64、65、97、98ページ〕）。しかし、グループには、委託先責任者が所属していないことがある（甲66、73）上、委託先責任者とされる者は、Cに対し、平成24年1月当初は指示などしていたものの、同年4月から数か月後の間は、週に2、3回しか多摩事務所に行っておらず、その後一切多  
20 摩事務所に行かなくなっていた（甲64）ところ、グループに所属せず、また、多摩事務所に居ない委託先責任者が委託先の従業員に対して指示をする方法につき、上記Lらは具体性のある供述をしていない一方、案件の進め方等につき、グループリーダーが指示をしていたとする前記(1)認定事実に沿うCの刑事公判廷における供述は、Cに自己の罪を免れるために虚  
25 偽の供述をする動機があるとの被告らの指摘を考慮しても、その内容が自然で、具体性に富んでいるため、採用することができるから、被告シンフ

フォームの社員によるCに対する直接の指示がなかったとする上記Lらの供述は、採用することはできないので、被告シンフォームの上記主張は採用することができない。

ウ 前記アの事情によれば、被告シンフォームとCとの間に実質的指揮監督  
5 関係が認められるというべきである。

(3) そして、本件個人情報、氏名、性別、生年月日、郵便番号、住所などといった情報であり、自己が欲しない他者に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り、これに対する期待は保護されるべきものであるから、本件個人情報は、原告らのプライバシーに係る情報として法的保護  
10 の対象となるものであり（最高裁平成29年10月23日第二小法廷判決・判時2351号7ページ参照）、Cは、故意に、本件行為によって、そのプライバシーを侵害したといえることができる。

(4) また、前提事実(4)及び(5)のとおり、Cは、本件パソコンにおいて、本件データベースに保管されている個人情報について、本件取得行為をしているので、本件取得行為は、本件業務に際してされたものである上、本件売却行為  
15 は、本件取得行為を契機とし、これと密接な関連を有すると認められるので、本件行為は、被告シンフォームの「事業の執行について」されたものに当たるといえる。

(5) 証拠（甲19の3、甲63、73）によれば、被告シンフォームは、Cから、業務上知り得た個人情報及び機密情報を開示、漏えいしない旨記載された「個人情報の取扱いに関する同意書」を受領しているほか、前記(1)認定事  
20 実ウのとおり、Cに対し、業務に従事する前に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実施し、その後も年1回情報セキュリティ研修を実施していたと認められるけれども、これらの事実だけでは、被告シンフォームがCの選任及び事業の監督について相当の注意をしたというには足りない。  
25

したがって、被告シンフォームは、Cの選任及び事業の監督について相当の注意をしたということとはできない。

(6) 小括

5 以上によれば、被告シンフォームは、別紙原告目録の判断欄に○と記載した原告らに対し、Cの本件行為による故意の不法行為について使用者責任を負うと認められる。

7 原告らの精神的損害の有無及び程度（争点(8)）について

被告シンフォームは、前記6のとおり、Cの故意による不法行為について使用者責任を負う。

10 そして、本件漏えい情報は、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、出産予定日又は保護者の氏名といった情報であるところ、このうち、氏名及び郵便番号・住所、電話番号、ファクシミリ番号又は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つては、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。そのため、これらの情報は、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これらの情報が流出することまでは欲しないものであるため、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に漏えいしたことへの不快感のみならず、それ  
15 による影響に対する不安感を生じさせるので、精神的損害が生ずるといえる。もつとも、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  
20 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、原告らは、本件漏えいでは、原  
25

告らについて、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、Cはイベントで集めた情報などとして本件売却行為をしており（甲89、乙90の1、2）、情報の量や質から被告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、本件漏えい情報は、情報一覧表の認定欄の情報項目の情報のおり原告それぞれでその範囲を異にし、また、その内容も異なる（氏名、生年月日、郵便番号、住所については、戸籍上のそれと同一でないもの又は現在のものとは異なるものが含まれ、また、性別、電話番号、ファクシミリ番号、メールアドレス及び出産予定日についても、内容が特定されていないため、正確でないものや現在のものと異なるものが含まれている可能性がある。）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を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快感・不安感につき、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、原告らは、未成年原告に関しては、不快感・不安感がこれから一生付きまとうなどとして、精神的苦痛は成年者とは異なると主張するけれども、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、個別の事情によることが大きい一方、自己の了知しないところで自己の個人情報が漏えいしたことへの不快感・不安感の程度は、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、同主張は採用することはできない。

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ある（甲49，50）上，本件漏えいの発覚経緯が，被告ベネッセらの顧客から，被告ベネッセに対し，被告ベネッセらと異なる通信教育事業者から被告ベネッセら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，被告ベネッセ  
5  
ら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（甲68，72）ことに鑑みると，本件漏えい情報も同通信教育事業者に流失した可能性があるといえるものの，原告らもダイレクトメールやセールス電話が原告ら全員に生じていることまでは主張しておらず，上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  
10  
以上に財産的損害その他の実害が原告らに生じたこととはうかがわれない。

一方，被告シンフォームは，前記6(4)のとおり，C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，C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，被告ベネッセの持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，  
15  
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（甲2，19の1から3まで），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円相当の本件謝罪品の交付を申し出るなどしている。

以上，本件に現れた一切の事情を総合考慮すると，別紙原告目録の判断欄に  
20  
○と記載した原告らにつき本件行為によ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，原告らが原告ら訴訟代理人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，別紙原告目録の判断欄に○と  
25  
記載した原告らにつき1人当たり300円の範囲内のものが本件行為による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。

8 以上によれば、被告シンフォームは、別紙原告目録の判断欄に○と記載した原告らに対し、Cを被用者とする使用者責任に基づき、それぞれ3300円の損害賠償債務を負うことができる。

#### 第4 結論

5 以上のとおり、原告らの被告シンフォームに対する請求は、別紙原告目録の判断欄に○と記載した原告らにつき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（第2事件原告については、同年12月9日）から支払済みまで年5分の割合による支払を求める限度で理由があり、原告らの被告シンフォームに対するその余の請求及び被告ベネッセに対する請求  
10 には理由がない。

東京地方裁判所民事第13部

裁判長裁判官 河 合 芳 光

15

裁判官 西 野 光 子

裁判官 土 屋 利 英

20