主　　文

1　被告らは，連帯して，原告甲に対し，２６９０円及びこれに対する平成２７年１月２９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　原告らのその余の請求をいずれも棄却する。

3　訴訟費用は，原告甲と被告らとの間では，これを２０分し，その１を被告らの，その余を原告甲の負担とし，原告乙及び原告丙と被告らとの間では，原告乙及び原告丙の負担とする。

4　この判決は，１項に限り，仮に執行することができる。

事　実　及　び　理　由

第１　請求

1　被告らは，連帯して，原告甲に対し，５万１６９０円及びこれに対する平成２７年１月２９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　被告らは，連帯して，原告乙に対し，３万円及びこれに対する平成２７年１月２９日から支払済みまで年５分の割合による金員を支払え。

3　被告らは，連帯して，原告丙に対し，１０万円及びこれに対する平成２７年１月２９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

以下の「民法」は，いずれも平成２９年法律第４４号による改正前のものである。また，以下，次のとおり表記する。

略語	もとの表記
原告甲	原告甲
原告乙	原告乙
原告丙	原告丙
被告ベネッセ	被告株式会社ベネッセコーポレーション
被告シンフォーム	被告株式会社シンフォーム

ベネッセホールディングス　　株式会社ベネッセホールディングス

丁　　丁

1　事案の骨子

⑴　主たる請求

被告ベネッセは，原告らの個人情報を含む顧客らの個人情報を管理し，平行して，被告シンフォームに対し，個人情報を分析するシステム（以下「本件システム」という。）の開発を委託した。被告シンフォームの委託先の従業員である丁は，上記各情報を，外部に漏えいさせた。

本件は，原告らが，これにより精神的損害を受けたなどと主張し，以下の根拠に基づき，損害賠償を求めた事案である。請求額は，原告甲につき５万１６９０円，原告乙につき３万円，原告丙につき１０万円である。原告らは，被告らの行為が共同不法行為であり，不真正連帯債務が成立すると主張する。

ア　被告ベネッセに対する請求（選択的）

不法行為（民法７０９条）（原告らの個人情報の管理に注意義務違反があったとの主張に基づく。）

使用者責任（民法７１５条１項本文）（丁による漏えい行為又は被告シンフォームの過失行為が被告ベネッセの事業の執行につきされたとの主張に基づく。）

イ　被告シンフォームに対する請求（選択的）

不法行為（民法７０９条）（被告シンフォーム自体に個人情報の管理に注意義務違反があったとの主張に基づく。）

使用者責任（民法７１５条１項本文）（丁による漏えい行為が被告シンフォームの事業の執行につきされたとの主張に基づく。）

⑵　附帯請求

各原告とも，附帯請求は，主たる請求に対する支払済みまでの民法所定の年５分の割合による遅延損害金であり，その初日は，平成２７年１月２９日（不法行為の後の日〔訴状送達の日の翌日〕）である。

２　前提事実（当事者間に争いのない事実並びに証拠〈甲１ないし５，２３，３１，３２，３９，６４，乙１７，９７，９８のほか後掲の各証拠〔特記のない限り，枝番の記載は省略する。〕〉及び弁論の全趣旨により容易に認定できる事実。別の訴訟の判決もあるが，認定に供した限度では，被告らからは，反対の主張立証がない。以下同じ。〉）

(1) 当事者

ア　原告らの身分関係

原告甲は，未成年者である原告丙の父親であり，原告乙は，原告丙の母親である。原告丙は，後記本件漏えい当時，３歳であった（甲８）。

イ　被告ベネッセによる個人情報の取得

被告ベネッセは，通信教育，模擬試験の実施や雑誌の発行・通販事業を行う株式会社であり，通信教育講座「こどもちゃれんじ」などを実施し，その顧客の個人情報（個人情報保護法２条１項１号）として，子供や保護者の氏名，性別，生年月日，住所，郵便番号，電話番号を，個人情報データベース（同法２条４項）として事業の用に供している個人情報取扱事業者（同法２条５項）である。

ウ　漏えいした個人情報

原告甲は，原告丙が被告ベネッセの上記通信教育講座を受講するに際し，少なくとも原告甲の漢字氏名，フリガナ，住所及び電話番号並びに原告丙の漢字氏名，フリガナ，生年月日及び性別（以下「本件個人情報」という。）を被告ベネッセに提供し，被告ベネッセは，これらの個人情報を事業活動に使用する目的で管理していた（甲５）。

エ　被告シンフォーム

被告シンフォームは，被告ベネッセのいわゆるグループ会社（被告らは，いずれもベネッセホールディングスの１００％子会社であり，以前は，被告シンフォームは被告ベネッセの１００％子会社であった。）であり，被告ベネッセから委託を受けてシステム開発・運用を行っている株式会社である。

オ　被告ベネッセによるシステム開発

被告ベネッセは，従前，主に，顧客管理のシステム及び販売管理のシステムに大別される複数のデータベースに顧客情報を集積して事業活動に活用していたが，事業の拡大に伴い，顧客情報が集積されているデータベースが大量になったため，平成２４年４月頃，そのリスク管理や上記の個人情報データベースを基にそれを統合して分析に用いるためのシステム（本件システム）を開発することとして，本件システム開発等の業務を被告シンフォームに委託した。

カ　丁

丁は，被告シンフォームの業務委託先の会社の従業員（システムエンジニア）として，平成２４年４月頃から，被告シンフォーム東京支社多摩事業所（以下「被告シンフォーム多摩事業所」という。）において，被告ベネッセの情報システムの開発等の業務に従事し，業務遂行の必要から，本件個人情報を含む被告ベネッセの受講者の個人情報及び開発中の本件システムのデータベース（以下，これらを併せて「本件データベース」という。）が記録された被告ベネッセのサーバコンピュータ（以下「本件サーバ」という。）に被告シンフォームから貸与された業務用パーソナルコンピュータ（以下「業務用ＰＣ」という。）からアクセスするための業務用アカウントを付与されていた。

(2)　本件漏えい

ア　本件漏えいの具体的方法

丁は，平成２６年６月１７日及び同月２７日に，被告シンフォーム多摩事業所内の執務室において，２度にわたり，業務用ＰＣを操作して，被告ベネッセの顧客情報が記録された本件サーバにアクセスし，合計約２９８９万件の受講者の個人情報のデータをダウンロードして業務用ＰＣに保存した上，これとＵＳＢケーブルで接続したＭＴＰ（Media Transfer Protocolの略。パーソナルコンピュータとスマートフォンなどの外部機器を接続する際の規格）に対応している自己のスマートフォン（以下「本件スマートフォン」という。）の内臓メモリ又はマイ

クロＳＤカードにこれを記録させて複製する方法により，上記顧客情報を領得した上，名簿業者に送信して売却した（以下「本件漏えい」という。）。

ＭＴＰは，携帯機器とパソコンとの間で，動画・音楽などのマルチデータを簡便に共有・連携するニーズに対応するために開発された規格であり，平成２３年１０月１８日に販売が開始されたＡｎｄｒｏｉｄ４．０をＯＳとするスマートフォンから搭載されるようになった。

イ　本件個人情報の漏えい

丁が漏えいした顧客情報のうちには，本件個人情報が含まれていた（甲５）。

ウ　本件漏えいの発覚等

被告ベネッセは，同年６月下旬頃，顧客からの問い合わせにより，被告ベネッセの顧客の情報が社外に漏えいしている可能性を認識したことから，調査を行い，丁が本件漏えいをしたことを特定し，同年７月１５日，本件漏えいについての刑事告訴を行った。丁は，同月１７日，警察に逮捕された。

被告ベネッセの持株会社であるベネッセホールディングス及び被告ベネッセは，同月９日及び同月１７日に記者会見をするなどして本件漏えいを公表し，その原因を徹底的に明らかにすると共に，被告ベネッセの顧客からの信用回復のため，事故調査報告書をまとめさせ，考え得る再発防止策を提言することを言明した。（甲２，乙４，８）

(3)　被告ベネッセによる事後措置

ア　金券の提供等

被告ベネッセは，同月１４日以降，漏えいの確認された顧客らにお詫びの文書を送付し，その後，漏えいの確認された顧客らの選択に従って，当該顧客らに対してお詫びの品として５００円分の金券（電子マネーギフト又は全国共通図書カード）を送付する方法又は漏えい１件当たり５００円を「財団法人ベネッセこども基金」（被告ベネッセが本件漏えいを受けて子らの支援等を目的として設立した基金）に寄付する方法による補償を実施した（甲１）。原告甲は，いずれの方

法も選択せず，被告ベネッセからの上記提案に応じることはできない旨の文書を返送した（甲８）。

イ　調査

ベネッセホールディングスは，同月１５日，その会長兼社長である戊の諮問機関として，本件漏えいに関する事実及び原因等の調査並びに再発防止策の提言を目的として，個人情報漏えい事故調査委員会（以下「本件調査委員会」という。）を設置した（甲２，３９）。

本件調査委員会は，事故調査報告書（最終報告書）を取りまとめ，同年９月１２日にベネッセホールディングスに提出し，被告ベネッセは，同月１７日，上記報告書を経済産業省に提出するとともに，同月２５日，本件調査委員会による調査報告の概要を公表した（甲２，３９）。

上記調査報告の概要には，「第２章　調査結果」の「Ⅲ　不正行為等の原因（不正行為を防げなかったシステムの問題点）」において，「1．不正行為等の原因となった情報処理システム」として，⑴アラートシステム，⑵クライアントＰＣ（業務用ＰＣ）上のデータのスマートフォンへの書出し制御設定，⑶アクセス権限の管理，⑷データベース内の情報管理が指摘され，次のとおりの記載がされている（甲２）。

㋐　アラートシステム

業務用ＰＣとサーバとの間の通信量が一定の閾値を超えた場合，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が採用されていたが，そのアラートシステムの対象範囲が明確に定められていなかったことなどから，丁による不正行為が行われた当時，業務用ＰＣと本件データベースとの通信を上記アラートシステムの対象として設定する措置が講じられていなかった。

㋑　業務用ＰＣ上のデータのスマートフォンへの書出し制御設定

被告シンフォームでは，業務用ＰＣを含む社内ＰＣ内のデータを外部メディ

アに書き出すことを禁止し，同行為を制御するシステム（セキュリティソフト）が採用されていたが，当該システム（セキュリティソフト）をバージョンアップさせる際に，特定の新機種のスマートフォンを含む一部の外部メディアへの書出しについて，書出し制御機能が機能しない状態が生じていた。

(ウ) アクセス権限の管理

被告シンフォームにおいては，付与済みのアクセス権限の見直しが定期的に行われていない状況が多く見受けられた。

(エ) データベース内の情報管理

被告シンフォームは，本件データベース内の個人情報をより細分化又は階層化しグルーピングした上で，異なるアクセス権限を設定する等の対策までは講じていなかった。また，本件データベースは，主としてマーケティング分析のために使用されていたが，その目的に照らして必要にして十分な程度までの個人情報の抽象化及び属性化は，行われていなかった。

３　争点及びこれに関する当事者の主張（なお，原告らのうち，原告乙は，平成２８年１月２０日の本件第６回弁論準備手続期日に出頭した後は，本件の口頭弁論期日にも弁論準備手続期日にも出頭しておらず，原告乙及び原告丙の主張は上記出頭した期日までの概括的な主張に限られるため，以下の具体的な主張（概ね平成２９年５月１０日付け原告ら準備書面(9)及び令和元年６月１４日付け原告ら準備書面(20)に基づくもの）は，いずれも原告甲に限って主張したものと認めるのが相当である。）

(1) 争点(1)（民法７１９条１項・７０９条〔対被告シンフォーム〕，同法７１５条〔対被告ベネッセ〕に基づく各請求）

本件漏えいについての被告シンフォームの過失の有無

【原告甲の主張】

ア　本件漏えいの予見可能性

(ア) 以下の各基準等からすれば，本件漏えいの当時，外部記録媒体へ個人情報を格納する方法による情報漏えいのリスクや，それを防止するための対策の必要

性，その対策として外部記録媒体の持込み自体を禁止するなどの方法の存在が，個人情報を取り扱う事業者において広く認識されている状況にあった。

ａ　旧通商産業省（現経済産業省）「情報システム安全対策基準」（平成９年。以下「安全対策基準」という。甲１３）は，情報システムの利用者が実施する対策項目を列挙し，「情報システムの運用に関連する各室の搬出入物は必要なものに限定すること」「搬出入物は，内容を確認し，記録をとること」との対策を要求していた。

ｂ　日本工業標準調査会「個人情報保護マネジメントシステム - 要求事項（ＪＩＳＱ１５００１：2006）」（平成18年。以下「ＪＩＳＱ１５００１」という。）及び旧財団法人日本情報処理開発協会（現一般財団法人日本情報経済社会推進協会）プライバシーマーク推進センター「ＪＩＳＱ１５００１：2006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」（平成２２年８月２５日。以下「マネジメントシステム実施ガイドライン」という。甲１９）においては，「事業者は，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管理のために必要かつ適切な措置を講じなければならない。」と規定し，その対策として，個人情報の取得・入力及び利用・加工の各場面において，外部記録媒体を接続できないようにすることが例示されていた。

ｃ　「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１０月９日厚生労働省・経済産業省告示第２号。以下「経済産業分野ガイドライン」という。甲１０）は，「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。）」が望ましいと規定されていた。

ｄ　独立行政法人情報処理推進機構（ＩＰＡ）「組織における内部不正防止ガイドライン」（平成２５年３月２５日。以下「内部不正防止ガイドライン」

という。甲１８）においては，「重要情報を取り扱う業務フロア内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ること」がリスクとして具体的に指摘されており，その対策として，重要情報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・利用を厳しく制限すること，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し，記録媒体等の利用は会社貸与品のみとすること，重要情報を扱う物理的区画内の行動についてはカメラ等で監視するとともに監視している旨を伝えることが記載されていた。

ｅ　日本データセンター協会「データセンターセキュリティガイドブックＶｅｒ１．０」（平成２５年８月２８日。以下「データセンターセキュリティガイドブック」という。甲２０）においては，データセンターにおけるＵＳＢメモリ等の情報記録媒体や携帯電話の持込み・持ち出し制限及び画像監視システムがセキュリティ対策として挙げられていた。

㈠　また，被告シンフォームは，毎年，正社員及び業務委託先の従業員の全員を対象とした情報セキュリティ研修を実施し，その中で，顧客情報の大量持出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出し制御が実施されている旨を周知させており（乙１７），大量の個人情報を保有するものとして，その対策の必要性を認識し，その徹底を指示していたのであるから，本件漏えい当時，スマートフォンが外部記録媒体として機能すること及びそのような手法による情報漏えいのリスクを十分把握していた。

㈡　丁が本件漏えいを行った際に使用した本件スマートフォンは，平成２４年１２月頃に発売が開始され，通信方式がＭＴＰであるスマートフォン（以下「ＭＴＰ対応スマートフォン」という。）であった。スマートフォン・タブレット向けオペレーティングシステム（ＯＳ）のうち，「ｉＯＳ」は，ＭＴＰに対応

しておらず，「Ａｎｄｒｏｉｄ」は，平成２３年5月１０日に公表された「Ａｎｄｒｏｉｄ３．１」において，ＭＴＰに対応した。平成２５年７月から同年９月までの３か月間のスマートフォン販売台数のＯＳ別シェアは，「Ａｎｄｒｏｉｄ」が５０．０％，「iＯＳ」が４７．２％であり，平成２６年７月から同年９月までのそれは，「Ａｎｄｒｏｉｄ」が６４．５％，「iＯＳ」が３１．３％であった。

また，代表的な商用セキュリティソフトがＭＴＰ使用制限機能に対応した時期は，平成１９年７月から平成２５年８月にかけてであった。

したがって，被告シンフォームは，本件漏えい当時，本件漏えいの方法で個人情報を不正に取得できることを予見できた。

イ　結果回避のための注意義務違反

被告シンフォームには，本件個人情報の漏えいを防止するため，以下のとおり，注意義務があったにもかかわらず，これを怠った過失がある。

㈠　私物スマートフォンの持込禁止に関する注意義務違反

被告シンフォームは，億単位の件数にのぼるベネッセ顧客情報を取り扱う企業であり，その顧客情報の中には，子供に関する個人情報も多数含まれるところ，前記ア㈠のとおり，種々のガイドラインにおいて，外部記録媒体の持込み制限がセキュリティ対策として挙げられている。よって，平成２６年当時には，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，それを防止するための対策の必要性，その対策として外部記録媒体の持込みを禁止する方法の存在が，個人情報を取り扱う事業者において広く認識されている状況にあった。そして，前記ア㈡のとおり，被告シンフォームは，毎年，正社員及び業務委託先の従業員の全員を対象とした情報セキュリティ研修を実施し，その中で，顧客情報の大量持出事例の紹介や，スマートフォンを含む外部記録媒体への書出し制御が実施されている旨周知していたというのであるから，被告シンフォーム自身，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

ンに顧客情報を導き出す手法による情報漏えいリスクを，十分に把握していた。

さらに，被告シンフォームの業務用ＰＣから本件データベース内の顧客情報にバッチサーバ経由でアクセスするには，テラターム（フリーソフト）が必要であったが，テラタームのインストール及びその利用は容易であったから，業務用アカウントを教示されている従業者であれば，テラタームをインストールすることにより容易に顧客情報にアクセスすることが可能な状況にあった。そうであれば，被告シンフォームとしては，アクセスした顧客情報をスマートフォン等に書き出すような事態が万が一にも発生しないよう，細心の注意を払うべきであった。

また，被告シンフォームにおいて，個人のスマートフォンを業務上利用させる必要性は，全くなかった。すなわち，電話やインターネット閲覧等が必要なのであれば，被告シンフォームにおいてそのための機器を別途準備すれば足りたし，私物の外部機器の持込みを制限することは，コストも手間もかからない最も容易かつ効果の絶大な不正対策であった。

以上のとおり，被告シンフォームには，私物スマートフォン等の持込みを禁止する措置を採るべき注意義務があったのに，私物スマートフォン等の持込みを禁止していなかった過失がある。

㈠ 業務用ＰＣに対するＵＳＢ接続禁止措置（ＵＳＢポートにＵＳＢメモリ等の外部記録媒体を接続することを禁止する措置）に関する注意義務違反

前記ア㈠のとおり，経済産業分野ガイドラインに「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，外部記録媒体を接続できないようにする。）」が望ましい措置であると規定され，内部不正防止ガイドラインでは，個人の情報機器や外部記録媒体を持ち込まれた場合の情報書出しのリスクを具体的に指摘した上，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。また，マネジメントシステム実施ガイドラインでは，取得・

入力及び利用・加工の各場面において，外部記録媒体を接続できないようにすることを，業務上の必要性に基づく限定対策として掲げている。このように，平成２６年当時には，外部記録媒体へ格納する（書き出す）方法による情報漏えいのリスクや，それを防止するための対策の必要性，その対策として外部記録媒体を接続できないようにする方法の存在が，個人情報を取り扱う事業者において広く認識されている状況にあった。

その上，上記㋐のとおり，被告シンフォーム自身，スマートフォンが外部記録媒体として機能することや，スマートフォンへ顧客情報を書き出す手法による情報漏えいリスクを十分に把握していた上，業務用アカウントを教示されている業務担当者であれば，容易に顧客情報にアクセスできる状況であったことからすれば，被告シンフォームとしては，アクセスした顧客情報をスマートフォン等に書き出すような事態が万が一にも発生しないよう，細心の注意を払うべきであった。

さらに，ＵＳＢポートを物理的に塞塞する器具は，遅くとも平成１７年には発売されており，これを使用することは情報漏えい対策として古典的かつ一般的なものであったから（甲２１），機密情報を扱う部署において，業務用ＰＣのＵＳＢポートに接続できる状態にしておくことはほとんどなかった。そして，ＵＳＢポートを物理的に塞塞したり，少なくとも接続を禁止するルールを設けたりすることは，コストも手間もかからない容易かつ効果的な不正防止対策である。

以上のとおり，被告シンフォームは，業務用ＰＣに対し，ＵＳＢ接続禁止措置を採るべき注意義務があったのに，ＵＳＢポートを物理的に塞塞する措置も採らず，また，業務用ＰＣにＵＳＢケーブルで接続することが社内で見られる光景であったにもかかわらず，漫然とこれを放置して，それを禁止するルールを設けなかった過失がある。

㋒　情報書出し制御措置・デバイス使用制御措置に関する注意義務違反

前記ア(ア)のとおり，内部不正防止ガイドラインでは，個人の情報機器及び外部記録媒体を持ち込まれた場合の情報持ち出しのリスクを具体的に指摘されていることからすると，平成２６年当時には，外部記録媒体へ格納する（書き出す）方法による情報漏えいのリスクや，それを防止するための対策の必要性が，個人情報を取り扱う事業者において広く認識されている状況にあったし，前記ア(イ)のとおり，被告シンフォーム自身，スマートフォンが外部記録媒体として機能することや，スマートフォンに顧客情報を書き出す手法による情報漏えいリスクを十分に把握していた。

ＭＴＰ方式の通信規格による情報書出しの危険性についても，本件当時までに具体的に言及した記事が公表されていたし，大手ベンダーを含むセキュリティ製品情報としての記事も公開されていた。本件当時，人気の高いスマートフォンの一つである「ＧＡＬＡＸＹ　ＳⅡ」の取扱説明書においても，パソコンとのデータ転送方式としてＭＴＰが明記されており，このような状況において，既にスマートフォン・スマートデバイスへのシフトやその危険性が議論されていた。そして，平成２４年１２月発売の一般消費者向け雑誌においては「スマホならより簡単なＭＴＰを使うとよい。」との記事も掲載されていた。したがって，ＭＴＰに限定したとしても，その対策が必要であることについて予見可能性があったことは，明らかである。スマートフォンあるいはＷＰＤからの情報漏えいについても同様である。

そして，丁が本件漏えいに使用した本件スマートフォンは，平成２４年１２月ころに発売が開始されたＭＴＰ対応スマートフォンであった。前記ア(ウ)のとおり，代表的な商用セキュリティソフトにおいては，既に平成１９年７月から平成２５年８月にかけて，ＭＴＰ使用制限機能に対応していたし，スマートフォン向けＯＳのうち，Ａｎｄｒｏｉｄについては，平成２３年５月１０日に公表されたＡｎｄｒｏｉｄ３．１においてＭＴＰに対応した。一方で，ｉＯＳについては，ＭＴＰに対応していなかったが，平成２６年当時，ｉ

ＯＳとＡｎｄｒｏｉｄそれぞれのシェアは，後者の方が大きかった。

よって，スマートフォンへ顧客情報を書き出す手法による情報漏えいリスクに対応するためには，ＭＴＰ使用制限機能のあるセキュリティソフトを業務用ＰＣに採用しておく必要があった。そして，代表的な商用セキュリティソフトは，全て平成２５年８月までにはそれに対応していた。

ところが，被告シンフォームは，業務用ＰＣにセキュリティソフトウェアを導入していたものの，平成２３年夏を最後に同ソフトウェアのバージョンアップを行っておらず，しかも，被告シンフォームが導入していたセキュリティソフトウェア「秘文」（株式会社日立ソリューションズ製，以下「本件セキュリティソフト」という。）は，ＭＴＰデバイスを含むあらゆるデバイスのすべてを制御する機能を有していたのに（甲４９），被告シンフォームがＭＴＰデバイスを制御の対象から外していたために，丁による顧客情報の領得を許容したものである。

以上のとおり，被告シンフォームには，本件漏えい当時，業務用ＰＣに搭載していたセキュリティソフトに備わっていたＭＴＰ使用制限機能を使用できる状態に設定する措置を採ることを怠った過失がある。

なお，被告らに要求されるセキュリティ対策の水準は，通常の企業に要求されるものではなく，被告らと同様の質・量の個人情報を扱い被告らと同様の企業規模の企業に要求される水準であり，クレジットカード会社や金融機関と同程度かそれ以上であるから，一般通常人を基準とすべきとの被告らの主張は，採用できない。

また，被告シンフォームは，既に導入していたセキュリティソフトの設定を変更すれば足りるから，費用は，かからない。結果回避義務があることも，明らかである。被告シンフォームのように，３年もの間更新すらしていないというのは，異常である。

㈡　アラートシステム設定に関する注意義務違反

前記ア㋐のとおり，内部不正防止ガイドラインは，個人の情報機器及び外部記録媒体を持ち込まれた場合の情報書出しのリスクを具体的に指摘しており，平成２６年当時には，外部記録媒体へ通信する方法による情報漏えいのリスクや，それを防止するための対策の必要性が，個人情報を取り扱う事業者において広く認識されている状況にあった。

その上，前記ア㋑で述べたとおり，被告シンフォーム自身，スマートフォンが外部記録媒体として機能することや，スマートフォンへ顧客情報を書き出す手法による情報漏えいリスク，ひいては顧客情報を大量に持ち出す事例が存在することを十分に把握していた。

被告シンフォームとしては，業務用ＰＣに接続した私物スマートフォンに顧客情報を書き出す手法により，本件データベース内の大量の顧客情報が漏えいする可能性が常に存していたのであるから，業務用ＰＣと本件データベース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，その通信を許容するかを確認するアラートシステムを設定すべき注意義務があった。ところが，被告シンフォームは，既存の連携システムのデータベースサーバについては，一定時間中にサーバと業務用ＰＣとの間の通信量が一定の基準値を超えた場合に，当該業務用ＰＣ使用者の所属長等に電子メールで確認を求めるアラートシステムを稼働させていたが，本件システム開発中のデータベースサーバに関しては，本格的運用開始前であったことを理由に，アラートシステムを設定していなかった過失がある。

㋓　監視カメラによる監視義務違反

前記ア㋐のとおり，内部不正防止ガイドラインでは，重要情報を扱う物理的区画のセキュリティ強化の対策として，カメラ等で監視するとともに監視している旨を伝えることが記載されていたし，データセンターセキュリティガイドブックでは　実施されるセキュリティ対策として，画像監視システム（監視カメラ）が挙げられていたから，平成２６年当時には，内部情報漏え

いのリスクや，それを防止するため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，個人情報を取り扱う事業者において広く認識されている状況にあった。

その上，前記ア㈠のとおり，被告シンフォームは，顧客情報の大量持出し事例を紹介するなど，情報漏えいリスクを十分に把握していたし，また，主要な入退出口には防犯カメラを設置していた。

被告シンフォームとしては，業務用ＰＣに接続した私物スマートフォンに顧客情報を書き出す手法により，本件データベースの大量の顧客情報が漏えいする可能性が高かったのであるから，情報漏えいを防ぐために，監視カメラ等により執務室を監視し，それを従業員等に伝えるべきであった。

以上のとおり，被告シンフォームには，監視カメラ等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があったのに，執務室の監視を行っていなかった過失がある。

【被告らの主張】

ア　総論

被告シンフォームには，本件漏えいについての予見可能性は認められず，次のとおり，結果を回避すべき注意義務違反も認められないから，過失はない。

イ　本件漏えいの予見可能性

ＭＴＰ対応スマートフォンを利用した個人情報流出のリスクについては，本件漏えい事件が発生するまで，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，注意喚起もされていなかった。また，ＭＴＰ対応スマートフォンに対する個人情報の書出しのリスクについて，本件漏えい事件が発生するまで，経済産業省等の行政機関や独立行政法人情報処理推進機構（ＩＰＡ）からの注意喚起は，一切なかった。本件漏えいの時点におけるＭＴＰ対応スマートフォンの国内シェアは，小さかった。本件漏えいの時点における商用セキュリティソフトのうち，実用的なＭＴＰ使用制御機能に対応したものは，ほとんどなかった。本

件漏えい事件によって初めて，スマートフォンを利用した個人情報不正取得の危険性が，認織されたのである。

被告シンフォームにおいても，本件漏えい以前に，クライアントＰＣから外部記録媒体に書出しがされ外部に情報が持ち出されるなどの事故やトラブルが発生したことはなく，特定の機種のスマートフォンに対して書出しができて個人情報が持ち出される可能性があるということを疑わせる事情は，一切なかった。そして，被告シンフォームは外部記録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導入していたため，執務室内の業務用ＰＣから情報が書き出されることはないという認識を有していた。

ウ　スマートフォンの持込み禁止に関する注意義務違反について

㈠　各基準について

ａ　安全対策基準

安全対策基準は，そもそも現代のセキュリティ状況や執務室を前提に策定された基準ではなく，本件漏えい当時，情報セキュリティの分野において，既に基準としての実質的意味を有していなかったものであり，被告シンフォームの注意義務の根拠たり得ない。また，安全対策基準中の「搬出入物」は，各自の身の回りの携行品・私物品を指すのではなく，業務上の必要性から，対象室（現在でいえば，サーバルームやデータセンターに相当するもの）内から搬出する設備や荷物等，あるいは搬入して設置する設備や荷物等を指している。また，安全対策基準では「搬出入物」の用語のほかに，「記録媒体」の用語も使用されているのであるから，「搬出入物」が「記録媒体」とは別の概念であることも，明らかである。なお，安全対策基準の最終改正がされた平成９年時点において，スマートフォンは，発売されていなかった。

したがって，原告甲が，安全対策基準で指摘する部分は，私物スマートフォンの持込み禁止措置を義務付けるものではない。

ｂ　内部不正防止ガイドライン

内部不正防止ガイドラインを定めたＩＰＡは，経済産業省の外郭団体にすぎず，内部不正防止ガイドラインは，対策例を紹介するにとどまり，法規範性を持たず，その中で紹介されている対策が実施されるべき法的義務として位置付けられていたものでもない。

また，内部不正防止ガイドラインは，「ＵＳＢメモリ等の記録媒体」と「スマートフォン等のモバイル機器」とを区別しており，「スマートフォン等のモバイル機器」については，重要情報格納サーバやアクセス管理サーバ等が設置されている「サーバルーム」のみを対象としてその持込み・利用を制限する運用を推奨していたのであって，「サーバルーム」以外の執務室等は対象としていなかった。

したがって，原告甲が，本件漏えい当時の内部不正防止ガイドラインで指摘する部分は，私物スマートフォンの持込み禁止措置を義務付けるものではない。

c　データセンターセキュリティガイドブック

データセンターセキュリティガイドブックは，そもそも執務室の情報セキュリティ対策の基準としてみるには不適当な性質のものであり，被告らの注意義務の根拠たり得ない。また，原告甲が，同ガイドブックで指摘する部分は，私物スマートフォンの持込み禁止措置を義務付けるものではない。

d　その他のガイドライン等

上記以外に，原告甲が手掛かりとするほかのガイドラインには，スマートフォンの持込み禁止について触れられていない。本件漏えい当時の基準として参考となりうるとすれば，経済産業分野ガイドラインの他にないが，これについては，平成２６年当時，私物スマートフォンの持込み禁止について，義務的事項として記載していなかったことはもちろん，望ましい事項としても何ら言及していなかったのであり，個人情報保護法上，私物スマートフォンの持込み禁止措置を採るべきことは，要求されていなかった。

(イ) また，「私物スマートフォン等の持込み禁止」は，本件漏えい当時，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かったほか，本件漏えい後においても，プライバシーマークやＩＳＭＳ認証（ＩＳＭＳ適合性評価制度〔国際的に整合性のとれた情報セキュリティマネジメントシステムに対する第三者認証制度〕に基づく認証）を取得しようとする企業や金融業界のシステムにおいてさえ，標準的なセキュリティ対策にはなっていなかった。

現在，セキュリティ意識の高い企業でも，私物スマートフォンの持込み制限をしていない理由は，このような措置が，これを徹底しない限りその実効性がない一方で，これを徹底すると業務阻害性が著しく高くなって現実的ではないという点にある。私物スマートフォンの持込み禁止は，現実的に考えて，一般の職場においては，個人情報の漏えい対策として採り得ない措置と言わざるを得ない。

エ　ＵＳＢ接続禁止措置に関する注意義務違反について

(ア) 各基準について

a　経済産業分野ガイドライン

本件漏えい当時，業務用ＰＣに対するＵＳＢ接続禁止措置については，経済産業分野ガイドラインにおいても，義務的事項として記載されていなかったばかりか，望ましい事項としても言及されていなかった。また，本件漏えい後に改訂された経済産業分野ガイドラインでも，上記措置は，「個人データを入力できる端末」において，望ましい事項として言及されたにすぎない。丁の使用する業務用ＰＣは，このような端末ではなかった。

b　内部不正防止ガイドライン

内部不正防止ガイドラインは，「スマートフォン等のモバイル機器」ないし「個人の情報機器」を業務用ＰＣに接続することを禁止しなければならないことを述べているのではなく，むしろ接続する場合があることを前提としているから，原告甲が内部不正防止ガイドラインに関して指摘する部分は，業務用ＰＣに対するＵＳＢ接続禁止措置を義務付けるものではない。

ｃ　マネジメントシステム実施ガイドライン

マネジメントシステム実施ガイドラインは，そもそも，法の要求事項を超えた高い保護レベルを前提とするから，法規範性を有しない。

(ｲ) 対策の一般性，有効性

本件漏えい当時，業務用ＰＣに対するＵＳＢ接続禁止措置を採っている企業は，ごく少なかった。本件漏えい後においても，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さえ，このようなセキュリティ対策をとっている会社は，数%程度しかなく，その他ほとんどの企業は，このようなセキュリティ対策をとっていなかった。そうすると，業務用ＰＣに対するＵＳＢ接続禁止措置が標準的な措置であったとはいえない。

また，ＵＳＢポートを物理的に塞塞する器具は取り外し可能であるし，パソコンには，マウスやキーボード，業務上利用されるＵＳＢ（被告シンフォームでは，一定の要件のもとに許可されたＵＳＢ）等を接続するためのＵＳＢポートが必要であって，全てのＵＳＢポートを塞塞できないから，結局のところ，ＵＳＢポートを物理的に塞塞することは，個人情報の漏えいに対する有効な対策とはならない。

オ　書出し制御措置に関する注意義務違反について

(ｱ) 各基準について

ａ　内部不正防止ガイドライン

内部不正防止ガイドラインは，前記のとおり，経済産業省の外郭団体であるＩＰＡが作成したものであって法規範性を有するものではなく，また，その名称からも明らかなとおり，組織における内部不正の防止を推進する目的で定められたものであり，その対象となる「内部不正」には，違法行為だけではなく，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も含まれているのであって，違法行為とはいえない行為をも広くその対象に含めた防止策を提示するものであるから，被告シンフォームの注

意義務の根拠たり得ない。

また，内部不正防止ガイドラインが言及するのは，個人情報機器及び外部記録媒体の業務利用及び持込みの制限であって，情報書出し制御措置については記載されていない。

b　その他ガイドライン等について

その他いずれのガイドライン等にも，本件漏えい当時，書出し制御措置について記載されていない。

(イ) 被告シンフォームの対策

また，本件漏えい当時，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あっても，書出し制御措置を採っていないものが過半であり，書出し制御措置は，標準的なセキュリティ対策にはなっていなかった。

そうした状況の中で，被告シンフォームは，平成１７年から，後記のとおり，その業務用ＰＣに導入していた本件セキュリティソフトにより，書出し制御措置を採っていたところ，本件漏えい当時，ＭＴＰ対応スマートフォンに対しては有効に書出しを制御することはできなかった。しかし，被告シンフォームとしては，外部記録媒体に書き出すことを技術的に制御する高度なセキュリティを導入していたため（被告シンフォームが導入していたセキュリティソフトは，ＭＴＰを含む，ＰＣにおいて使用される複数のデバイスについて，当該デバイスからＰＣへのデータの読取りも，ＰＣから当該デバイスへのデータの書出しもできないようにする機能を有していた。），被告シンフォームの執務室内の業務用ＰＣから情報が書き出されることはないという認識を有していた。それまで，その業務用ＰＣから外部記録媒体に対する書出しがされて外部に持ち出された等の，外部記録媒体に対する書出しが制御されていないことを疑わせるような事故やトラブルが発生したこともなければ，業務用ＰＣに充電のためスマートフォンを接続する従業員はそれまでにもいたにもかかわらず，スマートフォンに書出しができるといった報告がされたこともなく，特定の機種のスマ

ートフォンに対して書出しができて情報が持ち出される可能性があることを疑わせる事情は，一切なかった。被告シンフォームは，本件漏えい当時，本件セキュリティソフトにおいて，ＭＴＰ対応スマートフォンに対しては有効に書出しを制御することができなかったことを知りえなかった。この点について，原告甲は，代表的な商用デバイス制御ソフトにおいては，既に平成１９年７月から平成２５年８月にかけて，ＭＴＰ使用制限機能に対応していた（甲１２）と主張するが，そもそも本件漏えい当時，ＷＰＤ（ＭＴＰ）デバイスに対して使用制限機能を設定しなければ情報漏えいが発生するリスクがあるということは知られておらず，そのような危険を指摘する専門家もいなかったから，通常人（合理的な平均人）の一般的な水準に照らして，これに対応する措置を採っていなかったことによる過失責任は，生じない。なお，被告シンフォームは，当時，ＰＣに外部機器を接続することによって情報流出する場合に想定されていたのがＭＳＣデバイスであったことから，通信方式がＭＳＣであるスマートフォン，３．５型フロッピーディスク，リムーバブルディスク（ＵＳＢメモリ，MO，フラッシュメモリ，ＳＤメモリーカード及びスマートメディア等の外部記録媒体）等のリムーバブルメディアのほか，外付けハードディスク（ＵＳＢ接続，ＩＥＥＥ接続，ＰＣＭＣＩＡ接続及びＳＣＳＩ接続），ＣＤ及びＤＶＤについては，書出し制御措置を採っており，それらディスクへの書き込みを禁止することができた。

カ　アラートシステムに関する注意義務違反について

㈠　各基準について

ａ　内部不正防止ガイドライン

内部不正防止ガイドラインは，前記のとおり，法規範性を有するものではなく，また，違法行為とはいえない行為をも広くその対象に含めた防止策を提示するものであるから，被告シンフォームの注意義務の根拠たりえない。

ｂ　その他ガイドライン等について

その他いずれのガイドライン等にも，本件漏えい当時，アラートシステムについて記載されていなかった。

なお，本件漏えい後に，経済産業省が被告ベネッセに対して個人情報保護法に基づく勧告を行ったところ，同勧告は，「委託先（被告シンフォーム）において，今回の不正持ち出し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」ことに言及しているが，これは，同省が，個人情報保護法上アラートシステムを設定すべき義務があると解していることを意味するものではない。本来，アラートシステムを設置していないとしても個人情報保護法違反になることはあり得ないはずであるにもかかわらず，同省より，経済産業分野ガイドラインにおける記載と相反すると思われるような勧告が出されたのは，本件の社会的影響の大きさに鑑み，行政官庁として，個人情報保護に対する強い姿勢を打ち出す必要があるとの政策的判断によるものと思われる。

(イ) アラートシステムの一般性，有効性

本件漏えい当時，高度な情報セキュリティ対策をとっていた企業であっても，アラートシステムを採用していたものは少数であって，アラートシステムの設置が標準的に採られていた措置とはいえない。なお，本件漏えい後の現在であってさえ，プライバシーマークやＩＳＭＳ認証を取得するような企業であっても，アラートシステムを採用していないものが大半で，金融業界のシステムにおいてさえ標準的なセキュリティ対策にはなっていない。

また，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，その理由如何にかかわらず自動的に発令される仕組みであるため，一方で，その対象を広範に（すなわち閾値を低く）設定すれば，頻繁にアラートが発せられて，日常業務に支障が生じ，運用に耐えないものとなり，他方で，意図的に不正を働く場合には，複数回に分割してダウンロード又は通信することで予想される閾値を超えないようにすることが容易であり，個人情

報の漏えい対策としての実効性に乏しい。本件漏えい当時，本件データベースをアラートシステムの対象とすることはおよそ現実的ではなく，アラートシステムが設定されていなかったことは，見落としによるものではない。

キ　監視カメラに関する注意義務違反について

(ア)　各基準について

a　内部不正防止ガイドライン

内部不正防止ガイドラインは，前記のとおり，法規範性を有するものではなく，また，違法行為とはいえない行為をも広くその対象に含めた防止策を提示するものであるから，被告シンフォームの注意義務の根拠たりえないし，原告甲が，内部不正防止ガイドラインに関して指摘する部分は，執務室を想定しているものではなく，具体的措置についても「対策のヒント」という扱いであるから，監視カメラ等の画像による監視義務があることの根拠にはならない。

b　データセンターセキュリティガイドブック

データセンターセキュリティガイドブックでは，「画像監視システム」として「サーバー室内」での「画像監視システム」は「証跡としての役割を果たすことが挙げられます」とされ，侵入者や不正行為の監視・記録を目的とするとされる。これは，通常，人が出入りしない空間であることを前提にする画像監視システムであって，日々大勢の従業員が執務している執務室内への監視カメラ設置とは異なる目的のものであり，全く本件に適合していない。

(イ)　監視カメラの有効性

そもそも監視カメラは，常時，監視員が監視している場合でなければ，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あり，結局のところ，何かが起こった場合に，後から監視カメラを見て人の特定等をするために設置されるものである。また，執務室内で，従業員が業務用ＰＣに向かって業務をしているところが撮影されているとして，それが通常の業務をしているのか，

あるいは情報を不正に閲覧や保存等をしているのかは，外形的に変わらないから，業務用ＰＣからの個人情報の漏えいを防止するために監視カメラを設置してもほとんど実効性はない。さらに，執務室内への監視カメラの設置は，従業員に対して不快な思いを生じさせかねず，プライバシーの侵害ではないかなどと問題視される可能性もないとはいえないというデメリットもある。

そして，本件漏えい当時，高度な情報セキュリティ対策を採っていた企業であっても，執務室内に監視カメラを設置していたものは少数であって，このような措置が標準的に採られていたとはいえない。本件漏えい後の現在であってさえ，プライバシーマークやＩＳＭＳ認証を取得するような企業であっても，執務室内に監視カメラを設置していないものが大半で，標準的なセキュリティ対策にはなっていない。

なお，被告シンフォームでは，入退室管理の一環として執務室を含む施設の出入口に監視カメラを設けていたほか，執務室内についても，おおむねその全体を見渡せる位置に監視カメラを設けていた。

ク　まとめ

以上のとおりであるから，被告シンフォームには，本件漏えいについての予見可能性がなく，また，本件漏えいを回避することについて注意義務違反（過失）は，認められない。

(2)　争点(2)（民法７１９条１項，同法７０９条の各請求）

本件漏えいについての被告ベネッセの過失の有無

【原告甲の主張】

前記(1)の原告甲の主張と同様の理由で，被告ベネッセには本件漏えいによって原告甲に損害を生じさせたことについて過失がある。

ア　本件漏えいの予見可能性

争点(1)の原告甲の主張アに同じ。

イ　被告ベネッセには，本件個人情報の漏えいを防止するため，以下のとおりの

注意義務があったにもかかわらず，これを怠った過失がある（各主張はいずれも選択的）。

(ア) 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

個人情報保護法２０条は，「個人情報取扱事業者は，その取り扱う個人データの漏えい，滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。」と規定し，経済産業分野ガイドラインは，「講じなければならない事項」として，「個人データの安全管理措置を講じるための組織体制の整備」を掲げている。

また，内部不正防止ガイドラインは，「(2) 統括責任者の任命と組織横断的な体制構築」の項で，「内部不正の対象となる重要情報は組織内の多岐にわたる部門に存在するため，組織横断的な管理体制が構築できないと，組織として効果的・効率的な対策や情報管理ができないだけでなく，対策や情報管理が徹底されないおそれがあり，対策や情報管理が徹底されていないと，内部不正が発生してしまう危険がある」旨をリスクとして具体的に指摘し，対策のポイントとして，組織横断的な管理体制の構築では，統括責任者が対策実施の管理・運営の要員として各部門の部門責任者や担当者を任命することなどを求める。

さらに，実際上も，個人情報を取り扱うにあたって，利用・管理の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，取扱いや管理が杜撰となって流出や漏えいが生じる蓋然性が高まることは容易に認識し得る上，被告ベネッセの事業規模からすれば，同部門を設置することは，可能，かつ，容易なことであった。

そして，被告ベネッセが取得した顧客情報は，極めて大量である上，慎重な取扱いが求められる情報が含まれることや，本件システムの開発業務を被告シンフォームに委ね，被告シンフォームが同業務の一部をさらに第三者に委託し被告ベネッセの顧客情報に接触する者が別会社の従業員を含め多岐にわたる状況，さらには，後記のとおり，被告ベネッセには顧客情報の取扱いの委託先に

対して必要かつ適切な監督を行わなければならない義務があること等に鑑みれば，被告ベネッセには，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があった。

しかし，被告ベネッセは，顧客情報の利用・管理に責任を持つ部門を設置せず，ＩＴ戦略部などのいくつかの部門が本件データベースに関与し，各部門間の責任の所在や管理の方法が不十分となっており，このことが，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の放置に繋がったものであるから，本件漏えいについて過失があった。

(イ) 私物スマートフォンの持込禁止に関する注意義務違反

被告ベネッセは，本件システムの開発・運用を被告シンフォームに委託していたものの，元々が被告シンフォームの親会社であったものが，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があり，被告シンフォームの役員に被告ベネッセの役員が就任していた状況からすると，被告ベネッセは，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から，被告シンフォームと一体となって，組織的な事業として本件データベースを管理し，本件システムの開発を行い，顧客情報を取り扱っていたものと評価できる。

そうすると，被告ベネッセ自身が，私物スマートフォンの持込み禁止措置義務，業務用ＰＣに対するＵＳＢ接続禁止措置義務，情報書出し制御措置義務，アラートシステム設定義務及び監視カメラ設置義務を負うにもかかわらず，これらの注意義務を怠ったのであるから，本件漏えいについて過失があった。

(ウ) 委託先の選任及び監督に関する注意義務違反

被告ベネッセは，本件データベースの管理及び本件システムの開発や保守管理を被告シンフォームに委託していたところ，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。」と規定しているのであるから，被告ベネッセは，個人情報保護法上，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。

したがって，被告ベネッセは，被告シンフォームから契約内容の遵守について定期的に報告を受けたり，被告シンフォームに対して不定期に立入検査を行ったりするなどにより，当該契約内容が遵守されているかどうかを監督しなければならない。また，再委託や再々委託が行われていたから，そのような再委託等を禁止したり，再委託先等を限定したり（プライバシーマークを取得しているものに限る等），委託先が再委託先等に対して必要かつ適切な監督を行っているかも監督しなければならない。

そして，経済産業分野ガイドラインによれば，「必要かつ適切な監督」には，委託先を適切に選任すること，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ものとされ，ＪＩＳＱ１５００１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また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任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任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。」，「事業者は，次に示す事項を契約によって規定し，十分な個人情報の保護水準を担保しなければならない。a　委託者及び受託者の責任の明確化　b　個人情報の安全管理に関する事項　c　再委託に関する事項　d　個人情報の取扱状況に関する委託者への報告の内容及び頻度　e　契約内容が遵守されていることを委託者が確認できる事項　f　契約内容が遵守されなかった場合の措置　g　事件・事故が発生した場合の報告・連絡に関する事項」等

と規定し，マネジメントシステム実施ガイドラインでは，「審査の項目とその着眼点」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」等を例示していた。

これに，前記のとおり，被告ベネッセが取得した顧客情報は，極めて大量である上，慎重な取扱いが求められる情報が含まれること等を併せ考慮すれば，被告ベネッセは，業務委託先を選任するにあたって適切に個人情報を管理する体制にある業者を選任する義務とともに，その選任された委託先において，個人情報保護法２０条の安全管理措置が適切に運用されているかを監督する義務を負っていた。

しかし，被告ベネッセは，被告シンフォームが，本来，私物スマートフォン等の持込み禁止措置，業務用ＰＣに対するＵＳＢ接続禁止措置，情報書出し制御措置，アラートシステム設定及び監視カメラによる監視を行うべきであるにもかかわらず，それを怠り，適切に個人情報を管理する体制を講じていなかったことを知りながら，または少なくとも過失によりこのような体制であることを把握せずに委託先に被告シンフォームを選任した。

また，被告ベネッセは，被告シンフォームとの間で，個人情報の取扱いに関して契約書等を取り交わし，ミーティングを行うなどの形式的な管理体制を整えていたものの，被告シンフォームによる被告ベネッセの顧客情報の具体的な取扱い状況について正確に把握していなかった。そのため，被告ベネッセは，被告シンフォームにおいて，私物スマートフォンの持込み禁止措置，業務用ＰＣに対するＵＳＢ接続禁止措置及び情報書出し制御措置が採られていないこと，アラートシステムの対象範囲の設定が適正に行われていないこと，執務室の監視もされていないことを把握しておらず，そのような状況を改善するなどの対応をしなかった。

したがって，被告ベネッセは，以上のような被告シンフォームの不十分な情

報セキュリティ管理の実態を把握することなく，同社を委託先として選任し，さらに被告シンフォームによる再委託などを許していた結果，数社の派遣会社を経て，結局は，どこの会社の従業員であるのかも分からない丁に重要な個人情報であるデータについて，保管システムのアクセス権限を与えていたものであるから，被告ベネッセには，本件漏えいについて委託先の選任及び監督に関する過失があった。

ウ　以上によれば，本件システム開発は，被告ベネッセと被告シンフォームが一体となって取り組んでいた事業であり，個人情報の管理・運用において，事業としての一体性が認められるところ，被告ベネッセは，監督義務違反等の個別の義務違反に基づき，固有の不法行為責任を負うもので（民法７０９条），当該不法行為は，被告ベネッセが保有・管理していた個人情報を被告シンフォームに利用させたことによって生じたものであって，客観的に関連していることが明らかであるから，被告ベネッセと被告シンフォームは，共同不法行為者としての責任を負うことになる（民法７１９条１項）。

【被告ベネッセの主張】

被告ベネッセには，本件漏えいについての予見可能性はなく，結果を回避すべき注意義務違反も認められないから，過失がない。

ア　本件漏えいの予見可能性について

争点(1)の被告らの主張イに同じ。

イ　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

被告ベネッセは，個人情報保護の最高責任者としてＣＰＯ（Chief Privacy Officer〔最高個人情報責任者〕）を選任し，その配下に，全社的な個人情報保護活動を推進する専門部署である個人情報保護課を設置していたから，原告甲の主張は，その前提を欠くものである。

また，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は，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づけていた

としても，それを設置しなかったことが第三者（顧客等）に対する私法上の義務違反となるものではなく，また，そもそも，個人情報保護法上，「個人データの安全管理措置を講じ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，顧客情報の利用・管理に責任を持つ部門を設置することまで義務付けられているものではない（経済産業分野ガイドライン上も，あくまで望ましい手法にとどまる。）。このような部門の不設置と本件漏えいとの間の相当因果関係は，認められない。

ウ　私物スマートフォンの持込み禁止に関する注意義務違反等について

法人格が異なる者については別個独立の権利義務の主体として取り扱うべきであり，例外的に，厳格な要件のもとで法人格否認の法理によって，事案解決に必要な限度で法人格が否定されることがあるに過ぎない。原告甲が根拠として挙げている事情は，我が国のグループ企業内ではごく普通のものであり，そのような事情があるからといって法人格が否認されることはあり得ないから，仮に，被告シンフォームが私物スマートフォンの持込みに関する注意義務を負うとしても，被告ベネッセが同様に注意義務を負うということはできない。

エ　委託先の選任及び監督に関する注意義務違反について

㈠　そもそも，被告シンフォームにおいて，原告甲が主張する各措置を採るべき義務（私物スマートフォンの持込み禁止に関する注意義務，ＵＳＢ接続禁止に関する注意義務，書出し制御に関する注意義務，アラートシステム設定に関する注意義務，監視カメラによる監視に関する注意義務）は存在しなかったから，被告シンフォームがこのような措置を採っていなかったからといって，被告ベネッセに委託元としての選任監督の注意義務違反はない。

㈡　被告シンフォームが本件漏えい当時採用していた情報セキュリティ対策は，社会的に高い水準の情報セキュリティ管理レベルを期待される，製造，流通，ＥＣ（電子商取引），金融の各業界において国内大手ないし国内を代表すると目される企業と比較しても遜色ないものであった。また，同対策は，当時にお

ける経済産業省ガイドラインの「2－2－3－2．安全管理措置（法第２０条関連）」において望ましいとされていた事項まで全て網羅しており，経済産業分野ガイドラインに適合する状況にあった。さらに，被告シンフォームは，本件漏えい時まで，ＩＳＭＳ認証を取得してその継続・更新を繰り返しており，情報セキュリティマネジメントシステムに関する第三者機関から，十分な情報セキュリティ体制を構築しているとのお墨付きも与えられていた。このように，被告シンフォームは，当時の経産省ガイドラインからしても，また，当時の情報セキュリティ対策の一般的な水準からしても，明らかに高度な水準で情報セキュリティ対策を整えていたものであり，被告ベネッセがこのような法人を委託先として選任したことにつき，注意義務違反はなかった。

㈣ 被告ベネッセは，本件漏えい当時，当時の経産省ガイドラインからしても，また，当時の情報セキュリティ対策の一般的な水準からしても，明らかに高度な水準で，委託先である被告シンフォームに対して，必要な監督を実施していた。

㈤ 被告ベネッセには，そもそも本件漏えいについて予見可能性がなく，注意義務がなかった。

オ 以上のとおりであるから，被告ベネッセには，本件漏えいについて予見可能性がなかったから，これを回避するについての注意義務（被告シンフォームに対する選任及び監督についての注意義務）違反は認められない。

カ 原告甲による被告ベネッセの不法行為（民法７０９条）及び被告シンフォームとの共同不法行為（同法７１９条１項）の主張は争う。

⑶ 争点⑶ア及びイ（民法７１５条の使用者責任に基づく請求）

ア 被告シンフォームは，丁による本件漏えい（不法行為）について使用者責任を負うか否か（争点⑶ア）

【原告甲の主張】

㈠ 被告シンフォームの使用者性

民法７１５条の要件である使用者関係の有無を判断するにあたっては，使用者責任の根拠に鑑み，丁に対して実質的な指揮・監督関係があるかどうかによって判断することになる。

本件においては，被告シンフォームと丁との間に直接の雇用関係はないが，丁は，システムエンジニアとして被告シンフォームに派遣され，被告シンフォーム多摩事業所で被告ベネッセの情報システムの開発等に関する業務に従事し，日常的に被告シンフォームの社員から指示を受けていた。また，被告シンフォームは，丁に対し，被告シンフォームの顧客分析課長等の許可を受けた社員を通じて業務用アカウントを教示し，また，業務用ＰＣを貸与し，業務のため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。このような具体的な事情からすれば，被告シンフォームは，本件システム開発に関する事業について，丁を実質的に指揮監督する関係にあったということができる。

㈠ 事業執行性

丁による本件漏えいは，被告ベネッセから被告シンフォームが委託を受けた本件システム開発等の業務を，被告シンフォーム多摩事業所において丁が行っている際にされた。丁は，本件データベースを業務上利用し，同データベースへのアクセス権限を広汎に付与されており，そのアクセス権限を用いて本件個人情報を入手した。そうすると，本件漏えいは，被告シンフォームの「事業の執行」に該当する。

㈡ したがって，被告シンフォームは，丁による本件漏えいについて使用者責任を負う。選任監督上の相当の注意をしていたとの被告らの主張は争う。

【被告シンフォームの主張】

㈠ 被告シンフォームの使用者性について

被告シンフォームとその委託先会社の間では，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をすることができることとされていた。そして，実際に，丁を含む委託先会社の要員に対する業務遂行上の指示・管理その他指揮命令は，委託先会社の指示命令者により行われたから，被告シンフォームは，丁を実質的に指揮監督する関係にはなかった。

(イ) 事業執行性について

システムの開発，運用及び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，そのシステムの開発等のために実際に当該システムにアクセスすることは，システムの開発，運用及び保守等を行う以上当然のことであり，そのことから受託業務の遂行が委託元の事業の執行であるかのような外観を当然に有することにはならない。丁による本件漏えいは，あたかも委託先会社における職務の範囲に属するかのような外観を有することがあったとしても，被告シンフォームにおける職務の範囲に属するような外観を当然に有することになるわけではない。

また，原告甲は，丁の不法行為として「・・・顧客情報を自己のスマートフォンに書き出して名簿業者に売却する行為」を主張している。しかし，このような行為は，そもそも被告シンフォームの事業ではあり得ないし，丁の職務の範囲内であることもおよそ考えられない。

(ウ) 選任監督上の相当の注意をしていたこと

本件において，被告シンフォームは，丁から，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たほか，丁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。このように，被告シンフォームは，同社と丁との関係に照らして選任監督上の相当の注意をしていた。

イ　被告ベネッセは，被告シンフォーム又は丁の不法行為について使用者責任を負うか否か（争点(3)イ）

【原告甲の主張】

㈠ 事業執行性

本件システムは，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にベネッセ顧客情報を統合して分析に使用するためのシステムであり，その開発業務は，被告ベネッセの「事業の執行」に該当する。

㈡ 使用者関係（実質的指揮監督関係）の存在

使用関係の有無は，実質的な指揮・監督関係の有無により判断される。

本件においては，被告ベネッセと被告シンフォームとの間の業務委託契約では，被告ベネッセが，被告ベネッセが行っている安全管理措置と同等の措置が被告シンフォームでも講じられるように監督することや，被告シンフォームが受託業務を再委託する場合には，事前に被告ベネッセの承諾を求めることとしていた。また，被告ベネッセは，被告シンフォームに対し，その従業員に対する研修等に関する指示を行っていた。

被告ベネッセは，月次で「アウトソーシングレポート報告会」を開催し，委託業務全般の進捗状況の確認を行うほか，規模の大きな開発・運用案件については週１回以上のペースで定例ミーティングを実施していた。

さらに，被告ベネッセは，被告シンフォームに本件システムを開発させるにあたり，被告ベネッセのＩＴ戦略部においてベネッセグループの情報システムを担当していた従業員を，平成２５年１月から平成２６年３月まで被告シンフォームのＩＴソリューション部の部長として兼務させていた（甲２５の１ないし４，乙１７）。

このような具体的な事情からすれば，被告ベネッセは，本件システム開発に関する事業について，被告シンフォームを実質的に指揮監督する関係にあったということができる。丁についても同じである。

【被告ベネッセの主張】

㈠ 被告ベネッセの事業の執行ではないこと

被告ベネッセは被告シンフォームに本件システム開発の業務を委託し（本件業務委託契約），被告シンフォームは同契約に基づいて業務を行っていたものであるから，それが委託元である被告ベネッセの業務を執行していたことにはならない。

(イ) 使用関係（実質的指揮監督関係）がないこと

被告ベネッセと被告シンフォームとの間の本件業務委託契約には，原告甲の主張で指摘される契約文言や事実関係が存するが，これらは，被告ベネッセが個人情報保護法上委託元に求められる委託先の監督を行ったものに過ぎず，民法７１５条の要件である指揮監督関係の根拠となるものではない。

それ以外の原告甲の主張も，上記の根拠となるものではない。

被告シンフォームと被告ベネッセは独立した法人であり，独立した組織のもと，独自の事業遂行を行っていたから，両者は，一体となっていたわけではない。

以上のとおり，被告ベネッセと被告シンフォームとの間に実質的な指揮監督関係があると認める余地はなく，被告ベネッセに使用者責任が成立することはない。

被告ベネッセと丁との間にも，実質的な指揮監督関係はない。

(ウ) 選任及び監督についての相当の注意について

なお，仮に，被告ベネッセと被告シンフォームとの間に使用関係が認められるとしても，被告ベネッセが被告シンフォームの選任及び監督について「相当の注意」（民法７１５条１項ただし書）をしていたといえる。すなわち，仮に，本件におけるような委託関係によって発生する程度の関わりをもって実質的な指揮監督関係があると認めるとするならば，委託先に対するものとして社会通念上適切な選任・監督があること，すなわち個人情報保護法上の委託先の選任・監督義務と同程度の水準をもって，相当な注意をしていたと評価されるべきである。したがって，被告ベネッセに使用者責任は成立しない。

(4) 争点(4)（全請求）原告らに生じた損害の有無及び数額

【原告らの主張】

ア　原告甲

被告らの上記共同不法行為等は，原告甲のプライバシーに属する本件個人情報につき名簿業者等の数十社に拡散させ，それによって不特定の者にいつ購入されていかなる目的でそれが利用されるか分からないという不安感・不快感を原告甲に生じさせるものであり，原告甲は，これによって，慰謝料５万円相当の精神的苦痛を受けた。

被告らが漏えいした情報は，個人識別のための基本情報のみならず，続柄も含まれており，これにより，家族関係が一定程度明らかとなる。家族関係の情報は，社会的差別の原因となりかねない家柄の情報に繋がり得るものであり，極めてセンシティブな情報であるといえる。

そればかりか，被告らが漏えいした情報により，被漏えい者の多くが，子どもの教育に熱心な（少なくとも関心がある）家族の構成員である可能性が高いという属性が明らかになっている。このような情報は，入手を欲する者にとっては，ターゲットを絞った効率的な営業活動等に利用できるから，極めて高い経済的価値を持つ一方，被漏えい者にすれば，営業活動の一環としての不招請な迷惑勧誘を受けることにつながる情報であり，通常開示を欲しない情報である。

さらに，現代においては，典型的なデータベースソフトウェアが把握・蓄積・運用・分析できる能力を超えたサイズのデータ（ビッグデータ）を企業間で共同利用・解析すること等により，一定の属性の者の行動や趣味嗜好，思想等の分析がされている。このようなビッグデータは匿名化がされていることが多く，本来特定の個人と結びつかないデータとなっているが，個人情報を照合することにより，個人が特定されるおそれがあり，基本情報の流出に過ぎない場合であっても，その流出は，個人の特定だけでなく，その者の行動や趣味嗜好，ひいては思想等の把握につながる可能性があるものである。

被告ベネッセが漏えいした個人情報の流出先は，報道によれば，平成２７年３月の時点で約５００社にもなっており，流出の範囲は極めて広いばかりか，もはやその回収が不可能な状況となっている。また，流出先からの再流出の懸念も大きい。

これにより，原告甲は，将来にわたり，個人特定や更なる個人情報の引出しが行われる不安はもとより，家柄が特定されたり，行動や趣味嗜好が把握される不安も付きまとうほか，不招請な営業行為を受けるリスクも絶えない状況になっている。

さらに，この情報により被漏えい者の小中高校等の入学・卒業や成人式などのイベントのある時期が特定され，今後とも長期間にわたり，不招請な勧誘を受ける危険性がある。

また，被告らが漏えいした本件個人情報は，続柄や電話番号にも及ぶため，所謂オレオレ詐欺のような個人情報を利用した詐欺の勧誘に使われたり，子供の誘拐にも利用されるおそれがあるから，被漏えい者の不安感は重大であるし，長期間継続することになる。

以上のような事情を踏まえれば，原告甲に対する慰謝料は，５万円を下ることはない。

また，原告甲は，平成２６年７月１２日付けで被告ベネッセ宛に漏えいした項目を確認するための内容証明郵便を送付し，その送料として１２６０円を要し，また，被告ベネッセからの「お詫び」として５００円相当の金券を用意する旨の案内に対する異議申立てを簡易書留で送付し，その送料として４３０円を要した。これらの合計１６９０円も，原告甲の損害として認められるべきである。

イ　原告乙

被告らの上記共同不法行為等は，原告乙のプライバシーに属する本件個人情報につき名簿業者等の数十社に拡散させ，それによって不特定の者にいつ購入されていかなる目的でそれが利用されるか分からないという不安感・不快感を原告乙

に生じさせるものであり，原告乙は，これによって，慰謝料３万円相当の精神的苦痛を受けた。

ウ　原告丙

原告丙はまだ幼く，上記不安感・不快感がこれから一生つきまとい，学校の入学・卒業・受験などの多くの場面で業者に利用されるだけでなく，その幼さから犯罪の利用も警戒しなければならない。また，行政・病院・幼稚園などの公的団体を除くと，原告丙の個人情報を提供した団体は被告ベネッセが初めてであり，民間事業者に知らせた唯一の個人情報が漏れたことになるのであって，その不安感による精神的苦痛は，大人の比ではない。原告丙は，これによって，慰謝料１０万円相当の精神的苦痛を受けた。

【被告らの主張】

ア　本件漏えいの対象となった本件個人情報（続柄は含まれていない。）は，そもそも人が社会生活を営む上で他者に開示することが当然に予定されている個人識別情報であって，基本情報とされるものであり，プライバシーに関する情報の中で，その保護の程度は，最も低い。

イ　原告らには，本件漏えいにより，具体的損害，実質的損害は一切発生しておらず，また，住所や電話番号などの情報は変わることがあり得るものであり，実際，原告らは，本訴提起後，転居し，その住所及び電話番号の変更があった。そのため，本件個人情報は，原告らの現在及び将来の住所や電話番号を示すものではなく，原告らに具体的損害，実質的損害が将来発生する蓋然性もない。

本件漏えいにより，本件個人情報（基本情報）が流出したとしても，その流出先は名簿業者であって，また，必ずしも５００社に渡ったというわけではない。

原告らが，損害として主張するのは，抽象的な不安感や不快感に過ぎない。

プライバシーに関する情報が侵害されたことにより抽象的な不安感や不快感を抱く場合について，一律に損害を否定することはできないとしても，それらが違法として損害賠償の問題となるかは一般的平均的な人の感性を基準として判定さ

れるべきものである。そして，損害賠償制度は，損害の回復を目的とするものであるから，損害がないか，それが日常ありうる程度の軽微なものであれば賠償による救済の対象となりえない。

本件個人情報が名簿業者に漏えいしたことで想像される事態は，郵便，電話，メールという公共通信インフラを利用する接触形態によって勧誘等が行われることであるが，それは日常ごくありふれた行為で，そのような勧誘等は一般に許容されており，その事態をもって，不快感，不安が生じ，平穏な生活を送る利益が害されるとは，一般に考えられていない。また，事業者がする広告，宣伝物の送付，電話による勧誘は，事業者にとってはもちろん，消費者にとっても商品，役務についての知見を得，取引の便宜が図られる利益があり，ひいては取引機会の増大，経済の活性化の効用をもっているのであって，負の側面を強調することは正当ではない。結局，住所，氏名，電話番号といった情報の名簿業者への流出は，営業や宣伝に関する郵便物の増加や電話をもたらすことはあり得るが，それは，紙ゴミの増加又は一言半句の応答で足る負担をもたらす程度でしかなく，些細な不快があったとしても，日常ありうる程度の軽微なものということができる。それを超えた不快感，不安感を抱く人があるとすれば，それはその人にとっての主観的な不快感，不安であって，一般的平均的な人の感性を基準としたものを超えていると評すべきものである。

ウ　早稲田大学江沢民事件（最高裁平成１５年９月１２日第二小法廷判決・民集５７巻８号９１７３頁）は，プライバシーに関する情報が開示されたことによる具体的な損害の発生がないところで，精神的損害（慰謝料）発生を認めたものであるが，本件は，同事件と異なるから，精神的損害（慰謝料）を認めるべきではない。すなわち，早稲田大学江沢民事件では，本件と異なり，故意にプライバシーに関する情報が無断開示され，また，当該プライバシーに関する情報はより保護すべき必要性が高く，その開示について違法性が高いという特別な事情がある点で，本件とは全く異なるし，同事件の差戻審判決は，「本件個人情報の開示が違

法であることが本件訴訟において肯定されるならば，控訴人らの被った精神的損害のほとんどは回復されるものとも考えられる」とも判示するように実質的にはてん補されるべき損害の発生があるとは考えておらず，違法を宣伝する効果を与えるために名目的金額として損害を認定したと考えられている。本件のように，秘匿性が高くない情報が流出した事案において，流出による具体的な損害の発生がなく，抽象的な不安感・不快感のみが問題となる場合には，開示行為が故意である場合などを除き，慰謝料が発生する程度の精神的損害を認める必要はなく，また，流出後に行為者が相応の対応をとる場合には精神的苦痛は慰謝されるとみて，慰謝料の発生を認めるべきではない。

第３　当裁判所の判断

１　認定事実

前記第２の２（前提事実）のほか，後掲各証拠及び弁論の全趣旨によれば，次の事実が認められる。一部，前提事実を再掲する。

(1) 被告ベネッセ及び被告シンフォーム

ア　概説

被告ベネッセは，通信教育，模擬試験の実施や雑誌の発行・通販事業を行う株式会社である。被告シンフォームは，被告ベネッセのいわゆるグループ会社（被告らはいずれもベネッセホールディングスの１００％子会社であり，以前は，被告シンフォームは被告ベネッセの１００％子会社であった。）であり，被告ベネッセから委託を受けてシステム開発及び運用を行っている株式会社である。（前提事実(1)イ，エ）。

イ　被告ベネッセによる個人情報の取得と管理

被告ベネッセは，同社の講座等を利用する顧客から会員情報として個人情報の提供を受け，こうした情報をデータベースとして管理しており，これらの個人情報を，顧客に対する通信教育講座などの勧誘を目的とした手紙や電話等による情報提供のための営業情報として利用するなどしていた。

原告甲は，未成年者である原告丙が被告ベネッセの講座等を利用するに際し，被告ベネッセに対して本件個人情報を提供したもので，被告ベネッセが，同社の行う事業活動のために当該情報を利用することについては承諾していたと推認できる。

（甲３１，乙１７）。

ウ　新システムの構築

被告ベネッセは，従前，主として顧客管理のシステム及び販売管理のシステムに大別される複数のデータベースに顧客情報を集積して事業活動に利用していたが，事業の拡大に伴い，顧客情報が集積されているデータベースが大量になったことから，そのリスク管理等のため，平成２４年４月頃，別個に集積されていた顧客情報を統合してその分析に利用するシステム（本件システム）を構築することとして，本件システム開発等の業務を被告シンフォームに委託した（本件業務委託契約）（前提事実(1)オ）。

被告ベネッセは，本件業務委託契約において，被告シンフォームに対し，本件システム開発に必要な範囲で，本件個人情報を含む被告ベネッセが管理する個人情報について被告シンフォームの委託業者の従業員がアクセスすることを認めていた（甲３２）。

エ　被告シンフォームは，本件業務委託契約に基づいて委託された業務を，被告ベネッセの承諾を得て，複数の外部業者に分散して再委託し，再委託を受けた業者が，さらに別の業者に再々委託することを認めていた。そして，被告シンフォームは，これら再委託先等の業者の従業員（以下，これらの者を含めて，単に「業務委託先の従業員」ということがある。）が，開発業務上必要がある場合に，被告シンフォームが貸与した業務用ＰＣから本件データベースにアクセスすることを認めていた（甲３２，３９）。

もっとも，被告シンフォームは，本件システム開発業務を行っている従業員が，再委託先業者に所属する従業員なのか，再々委託先業者に所属する従業員である

のかといった，被告シンフォームとどのような契約関係にある会社の従業員であるのかを明確に把握しておらず，そのような従業員に対しても本件データベースに保存された個人情報等に広範囲にアクセスする権限を付与する場合があり，このため，業務委託先業者の担当者に対する業務の分配や，付与するアクセス権限を必ずしも適切にコントロールすることができていなかった（甲２・７頁）。

なお，丁を雇用した会社は，被告シンフォームから直接再委託を受けたのではなく，被告シンフォームとＡ社，Ａ社とＢ社，Ｂ社と丁を雇用した会社，という，順次の業務委託契約があったが，丁は，被告シンフォームに対し，丁が行っていた業務の内容や性質，丁が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提出し，本件システム開発業務を行うに際し，許可なく，被告ベネッセ及びその顧客の機密情報並びに個人情報に関する資料を外部に持ち出したりしてはならないことを約していた（甲３２〔１３頁〕，４８）。

(2) 本件漏えい

ア　丁の本件漏えい時の執務環境，私物スマートフォンの持ち込み，充電等

丁は，平成２４年４月頃から，被告シンフォーム多摩事業所において，本件システム開発等の業務に従事するようになった。このため，丁は，本件システムの開発，運用及び保守に関連する業務に従事する者として，本件システムやそれに連携される既存のシステム（以下「連携システム」という。）のデータベース内の顧客情報にアクセスするために必要なアカウントを教示され，かつ，被告シンフォームから貸与された業務用ＰＣを用いていた。

当時，被告シンフォーム多摩事業所の執務室内においては，丁を含む業務委託先業者の従業員が個人で所有する従来型の携帯電話やスマートフォンが日常的に使用されており，これらが，充電のために業務用ＰＣにＵＳＢケーブルで接続されることも行われていた。丁は，平成２５年７月ころ，充電目的で丁のスマートフォンを業務用ＰＣに接続したところ，スマートフォンへのデータの書出しが可能な状態にあることに気づいた。

（前提事実⑴カ，甲３２〔４頁〕，乙１７，９７）

イ　本件漏えいの実行

丁は，金銭的に窮し，平成２６年６月１７日及び同月２７日，被告シンフォーム多摩事業所の執務室内において，業務用ＰＣからバッチサーバ経由で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含む個人情報を抽出して業務用ＰＣに保存し，同ＰＣからＵＳＢケーブルを用いて丁所有の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態様により，本件個人情報を含む大量の個人情報を不正に取得した（前提事実⑵ア）。

ウ　丁による個人情報の使用

丁は，不正に取得した本件個人情報を含む上記個人情報を，名簿業者に売却した。丁は，上記日時における本件漏えいのほかにも，相当期間にわたって，顧客に関する個人情報を不正に取得した。これらも併せると，不正に取得した個人情報は，延べ約２億１６３９万件となり，同一人物と見られる個人情報を名寄せして重複を解消したとしても，約４８５８万人分という，大量のものであった。（甲２，３９）

⑶　本件スマートフォン

本件スマートフォンは，従来のスマートフォンの用いていた大容量ストレージ（ＭＳＣ）という通信方式とは異なり，ＭＴＰという通信方式に対応していた。

ＭＴＰは，デジタルカメラの画像転送プロトコルをベースに，音楽や動画ファイルなどを転送することを可能としたデータ転送の一つの規格であり，デジタルカメラやＩＣレコーダーなどに採用されており，ファイルシステムの管理は，これらデバイス側で行われる（ＭＳＣではパソコン側で行われる。）。そのため，本件スマートフォンがパソコン（ＷｉｎｄｏｗｓをＯＳとして使用）に接続されると，デバイスドライバや対応するアプリケーションソフトをインストールすることなく，ＷＰＤデバイスとして認識され，同デバイスにデータを転送することが可能となった（以下，通信方式にＭＴＰを採用するデバイスを，単に「ＷＰＤデバイス」ともい

う。）。

（甲１１）

⑷ 本件漏えい当時に被告シンフォームが採用していた安全管理措置

ア インターネットとの接点

被告シンフォームは，データセンターに設置されている本件サーバ（被告シンフォームが管理する被告ベネッセのサーバ）と被告シンフォームの執務室内の業務用ＰＣとの間を専用回線で繋いでおり，インターネット回線を使用しないこととした上で，やむなくインターネットと接する部分について，以下のとおり対策を実施していた。

㋐ ファイアウォールを導入し，必要最小限の通信のみ許可（申請ベースで変更）する通信制御を実施していた。

㋑ 不正アクセス検知は，外部業者に委託してリアルタイムで監視を行い，攻撃を検知し，かつ，システムに影響が出ると判断した場合は直ちにインシデント対応を実施することとしていた。

㋒ リモート接続について，申請制により最小限の人にのみ許可し，かつ，重要なシステムはアクセスできないという制御を実施していた。

㋓ インターネット接続が可能なＵＲＬについて，業務で必要なサイトのみ許可していた。

㋔ 社外への電子メールを全て保存していた。

（甲２，乙１，乙９７）

イ 物理的境界

個人情報が保管されている本件サーバは，隔離されたデータセンターに設置され，同室への入退室に対して厳しい管理（入館の事前申請・入館制限，私物持込み不可，機器持出し不可及び監視カメラ設置等）が行われていた。また，個人情報を取り扱う業務の執務室への入退室についても管理（申請制にて入退室制限，入退室記録保存，監視カメラ設置等）が行われていたが，個人所有のスマートフ

ォンの持込みや充電のために業務用ＰＣにＵＳＢケーブルを用いて個人所有のスマートフォンを接続することは，認容されていた。

（甲２）

ウ　内部ネットワーク

本件データベース内の領域が本番環境と開発環境に分離されて，個々の領域にアクセスするには，それぞれ別個に設定されたアカウントが必要であり，業務上必要なデータベースのみへのアクセスが可能なようにアクセス制御が行われるとともに，私物パソコンの社内ネットワーク接続が禁止され，全業務従事者個々人に対して，所定の設定がされた業務用ＰＣが貸与されており，その業務用ＰＣについても，セキュリティ目的で，アクセス及びダウンロードについて全てネットワーク通信記録を取得することによる監視が行われていた。

（甲２，乙１７）

エ　サーバ

本件サーバに関しては，アカウント管理が行われ，また「踏み台サーバ」（直接にサーバにアクセスさせないことにより，外部からの侵入リスクを軽減させるサーバ）としてバッチサーバを経由させた上で本件サーバにログインすることとし，これらについて個人が特定できる形でサーバへのアクセスログの記録が保管されていた。

業務用ＰＣと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閾値を超えた場合，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ようになっていたが，業務用ＰＣと本件データベースとの通信については，本件システム開発中であったことから，丁による本件漏えいの当時，上記アラートシステムの対象として設定する措置は，採られていなかった。

（甲２，乙１７）

オ　業務用ＰＣに対するセキュリティ対策

管理者業務で使用するパソコンとそれ以外の業務で使用する業務用ＰＣとを分け，担当者に対して専用のパソコンとして貸与し，それぞれ利用場所を制限していた。また，業務用ＰＣについて設定されていたセキュリティ対策としては，ウイルス対策ソフトの搭載，ＵＲＬフィルタリングツール（業務に必要なＵＲＬのみ接続を許可する。）の搭載，メールフィルタ（個人情報を記載したメールと判断されたものについての通信を差し止める。）の設定，その他標準として選定したソフトウェアの搭載と個人による標準仕様の変更の制限，パスワードの設定等があった。

（甲２，乙９７）

カ　セキュリティソフトによる書出し制御等

業務用ＰＣには，前記のほか，平成２１年６月３０日に発売されたセキュリティソフト「秘文Ｖｅｒ．９」（本件セキュリティソフト）が導入されていた。その主な機能は，操作ログの記録，ＵＳＢ等の外部記録媒体への書き込み制御，ディスク暗号化などであった。

本件セキュリティソフトは，リムーバブルメディア，ＣＤ，ＤＶＤ，外付けＨＤＤのほか，イメージングデバイス，ＷＰＤデバイス，その他の制御デバイスなどについて個々にその使用をできなくするように制御することが可能であった。

被告シンフォームでは，本件セキュリティソフトを平成２３年８月にバージョンアップさせる際に，業務用ＰＣ上のデータを外部記録媒体へ書き出すことを制御する機能の見直しを行い，通信方式がＭＳＣのスマートフォンを含む一部の外部記録媒体については制御する措置が採られていた。被告らは，これにより，業務用ＰＣからスマートフォン一般へのデータの書出しができなくなっていると理解していた。しかし，上記制御する措置は，通信方式がＭＴＰのＷＰＤデバイスについては採られていなかった（弁論の全趣旨〈被告準備書面２４ｐ４〉）。

被告シンフォームにおける本件セキュリティソフトのバージョンアップは，上記平成２３年８月の後，平成２６年７月までの間，行われなかった。

なお，被告シンフォームは，本件漏えい後，遅くとも平成２６年９月１７日までに本件セキュリティソフトの設定を見直し，スマートフォンを含む書出し機能を持つ可能性のある全ての外部メディアについて，業務端末からの書出しができない設定とした。

（甲２，１２，３９，４９，乙９７）

キ　顧客情報の機密指定，研修等

被告シンフォームでは，同社が取り扱う被告ベネッセの顧客情報を区分し，それらをそれぞれ機密情報として位置付けていた（被告ベネッセにおいても，本件個人情報を機密情報と位置付けていた。）。

また，被告シンフォームでは，就業の条件として，個人情報及び機密情報の開示，第三者提供，又は漏えい等を行わないことを誓約する内容の同意書の提出を求め，毎年，業務従事者（被告シンフォームの社員であるかどうかにかかわらない。）の全員を対象とした情報セキュリティ研修を実施し，セキュリティソフトによる外部記録媒体への書出し制御の実施等の告知を行うなどして，個人情報や機密情報の漏えい防止のための注意喚起等を行った上，研修内容を踏まえたテストを実施していた。

（甲２，乙１７）

２　本件個人情報の被侵害利益性及び丁の不法行為責任

⑴　本件個人情報の被侵害利益性

本件漏えいによって流出した本件個人情報の内容は，原告甲の漢字氏名，フリガナ，住所及び電話番号並びに原告丙の漢字氏名，フリガナ，生年月日及び性別である（前提事実⑴ウ）。

なお，原告甲は，原告甲のメールアドレスや原告甲と原告丙の続柄も漏えいした旨主張するが，これらも漏えいしたと認めるに足りる証拠はない。

まず，原告甲の住所，電話番号は，原告丙が本件漏えい当時３歳の未成年者であったことからすると，原告丙自身の住所，電話番号でもあると推認できること，そ

の他のそれぞれの漢字氏名，フリガナ等も，原告甲及び原告丙の家族関係を表す情報といえることから，本件個人情報全体が原告甲及び原告丙の個人情報であると認められる。なお，これらを照らし合わせれば，原告甲と原告丙の続柄も容易に推測できるから，この点も漏えいしたのと同視できる。

そして，本件個人情報は，これを全体としてみれば，原告甲及び原告丙のプライバシーに関する情報として法的保護の対象となるというべきである（最高裁平成２９年１０月２３日第二小法廷判決及び最高裁平成１５年９月１２日第二小法廷判決・民集５７巻８号９７３頁参照）。

もっとも，原告乙についての個人情報そのものが明らかになったことを認めるに足りる証拠はない。原告乙が原告甲及び原告丙の同居の家族であることを考慮しても，本件個人情報が原告乙の関係でもプライバシーに関する情報として法的保護の対象となるということはできない。

⑵　丁の不法行為責任

丁は，平成２６年６月当時，被告シンフォームの業務委託先の従業員であり，同月，被告シンフォームが被告ベネッセから提供を受けてその業務に使用する目的で管理していた本件個人情報を，故意に，名簿業者に売却する意図のもとに不正に取得し，他の個人情報と一括して名簿業者に売却したから，原告甲及び原告丙のプライバシーとして法的保護の対象となる利益を違法に侵害したと認められる。

丁は，原告甲及び原告丙に対し，それぞれ，損害が認められる限り，本件漏えいにつき，不法行為による損害賠償責任を負う。

３　争点⑴（本件漏えいについての被告シンフォームの過失の有無）について

⑴　本件漏えいの予見可能性について

ア　予見可能性を肯定する事情

㋐　通信方式がＭＳＣである従来型のスマートフォンに関する認識

前提事実⑶イのとおり，本件調査委員会の事故調査報告書には，本件漏えい当時，外部メディアへの書出し制限がされていた旨記載されていた。証拠（甲

１０，１３，１８，１９，２０，６０，６１）によれば，本件漏えい以前に，複数の文献等が外部メディアへの書出しの危険性を指摘していたと認められる。

これらのことからすると，被告シンフォーム自身も，本件漏えい当時，少なくとも，ＭＴＰに対応していない通信方式のスマートフォン（通信方式がＭＳＣである従来型のスマートフォン）については，それが業務用ＰＣのＵＳＢポートに接続されることにより個人情報を不正に取得される可能性があることを認識していたことが認められる。

⑷ 本件漏えい当時のＭＴＰ対応スマートフォンに関する認定事実

各項末尾等に記載した証拠及び弁論の全趣旨によれば，以下の事実が認められる。

ａ　国内のスマートフォン利用者は，平成２４年１１月には，２４００万人を超えていた。スマートフォンの出荷数は，平成２５年で約２９２５万台，平成２６年で約２７７０万台であった。スマートフォンの契約件数は，平成２５年３月末では約４０００万件，平成２６年３月末では約６０００万件であり（乙３８資料１），平成２５年３月以降，ＯＳが「Ａｎｄｒｏｉｄ」であるスマートフォンが全体の約４０パーセントであった。スマートフォン全体のうち「Ａｎｄｒｏｉｄ４．０」以上のバージョンの「Ａｎｄｒｏｉｄ」端末（ＭＴＰ対応スマートフォン）が占める割合は，平成２５年６月時点で１９．８８パーセント，平成２６年６月時点で２１．４１パーセントであった。（甲５４，乙３８，７７）

ｂ　通信方式がＭＴＰである機器は，ＰＣのウインドウズ上ではＷＰＤデバイスとして扱われるので，ＭＴＰ対応機器の使用制限は，ＷＰＤデバイスの使用を制限する設定とすることで可能となる。当時の一般的なセキュリティソフトがＷＰＤ使用制限機能に対応した時期は，概ね別紙のとおりであり（ただし，エムオーテックス（株）は平成２５年１０月から〈乙３９〉），被告らが使用していた「秘文Ｖｅｒ９」（本件セキュリティソフト）においては，

平成２１年６月であった。本件セキュリティソフトにおいては，ＭＴＰ制御機能として，未登録デバイスの使用制御ができた。

（甲１２，４９，５０，乙３９）

ｃ　「Ａｎｄｒｏｉｄ４．０」より前のバージョンの「Ａｎｄｒｏｉｄ」端末（いわゆる旧機種）には，平成２４年７月から同年１１月までに，「Ａｎｄｒｏｉｄ４．０」へのバージョンアップがキャリアから提供されており，その頃発行された大手パソコン雑誌において，ＭＳＣ以外にＭＴＰによる通信方法が紹介されていた。

また，同時期に，日本電気株式会社がスマートデバイス（スマートフォンとタブレット端末）のＭＴＰ等の利用の制限といったセキュリティの強化を勧める講演を行い（甲５６），ＷＰＤデバイスの制御機能を有することを明示したセキュリティソフトの記事がネット上で公開されていた。

（甲５５，５６，６３）

㈢　検討

被告シンフォームは，被告ベネッセから委託された本件システム開発等の業務について，他社に対して再委託を行い，それらの会社による再々委託を認め，これら業務委託先の従業員に対し，業務上の必要に応じて，業務用ＰＣから本件個人情報を含む大量の個人情報にアクセスすることを認めていたうえ，これらの業務委託先の従業員が，被告シンフォーム多摩事業所の執務室内に私物のスマートフォンを持ち込んで業務用ＰＣにＵＳＢを接続して充電を行うこともあり，これを容認していたと推認できる。このような状況からすれば，そのような従業員の中には，ＭＴＰ対応スマートフォンを使用する者がいるであろうことを認識し，あるいは認識可能であったと推認できる。

また，被告シンフォームは，本件漏えいの時点（平成２６年６月時点）において，通信方式がＭＳＣである外部機器（スマートフォンを含む。）については，業務用ＰＣのＵＳＢポートに接続して個人情報を不正に取得する可能性を

認識していたといえる。そして，前記認定によれば，当時，相当数のＭＴＰ対応スマートフォンが国内市場に出回っていたと推認されるのであるから，執務室内で作業する従業員が，ＭＴＰ対応スマートフォンを執務室内に持ち込んで，業務用ＰＣのＵＳＢポートに接続することにより，個人情報を不正に取得する可能性があることを認識し得たことが，推認できる。

イ　被告らの主張の検討

被告らは，①本件漏えいの時点におけるＭＴＰ対応スマートフォンの国内シェアは小さかった，②本件漏えいの時点におけるセキュリティソフトのうちＭＴＰ使用制御機能に対応したものは皆無であった，③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不正取得の危険性が認識されたから，被告シンフォームには本件漏えいについての予見可能性は認められない，④被告らは，パソコンに関しては，一般ユーザーである旨主張する。

㈠　①について

前記ア(イ)ａのとおり，ＭＴＰ対応スマートフォン（「Ａｎｄｒｏｉｄ４．０」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２５年６月時点で１９・８８％，平成２６年６月時点で２１・４１％であったほか，平成２６年３月末のスマートフォンの契約数は，約６０００万件であった。平成２５年１月から平成２６年６月までの出荷台数を前提に計算すれば，平成２６年６月頃のＭＴＰ対応スマートフォンの台数は，約９００万台（≒〈２９２５万台＋２７７０万台÷２〉×０．２１４１）となり，この期間に出荷されたものがすべてそのまま平成２６年６月に使われていたわけではないとしても，当時，多数のＭＴＰ対応スマートフォンが使われていたと推認できる。そして，前記ア（イ）ｂにおいて認定したとおり，当時の一般的なセキュリティソフトがＷＰＤ使用制限機能に対応した時期が概ね別紙のとおりであったことなどからすると，本件漏えいの時点におけるＭＴＰ対応スマートフォンの国内シェアは小さかったとする被告ベネッセの主張を考慮しても，被告シンフォ

ームが，ＭＴＰ対応スマートフォンを業務用ＰＣのＵＳＢポートに接続することにより個人情報を不正に取得される可能性があることを認識し得たという前記判断が左右されるとはいえない。

(イ) ②について

証拠（乙３９・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）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（ハミングヘッズ株式会社）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，同報告においては，「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業務用ＰＣ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。本件全証拠によっても，本件システムにおいて，デジタルカメラ等を含めたＷＰＤデバイスから業務用ＰＣにデータを転送する必要があったとは認められないから，読み取り専用でなく双方向のデータのやりとりを不可としてもよいと考えられる。本件との関係では，上記定義に該当するような設定ができないことを理由に，実用的でないと評価するのは，相当でない。そして，上記調査報告の添付資料によっても，被告らが導入していた「秘文Ｖｅｒ９」は，平成２１年６月からデバイスの使用制御が可能であったとされ，その国内市場シェアは１７．８パーセントと２番目に大きなものであった。なお，平成２６年６月当時，国内シェアが１８．８パーセントと最も大きいエムオーテックス株式会社の「ＬａｎＳｃｏｐｅＣａｔ」も特定ユーザー向けの個別カスタマイズ機能として平成２５年１０月

から同報告が実用的とするＭＴＰ制御機能を搭載することができたし，平成２７年１月からは同機能を標準で搭載したとされている。また，国内シェアが５．４パーセントと４番目に大きいクオリティソフト株式会社の「ＱＮＤ」も上級パッケージには標準でデバイス制御機能が搭載されていたし，４．１パーセントと５番目に大きい日本電気株式会社の「ＩｎｆｏＣａｇｅ　ＰＣセキュリティ」もデバイスの使用制御機能を有していたとされている。そして，通信方式がＭＴＰである機器はＰＣのウインドウズ上ではＷＰＤデバイスとして扱われるので，ＭＴＰ搭載機器を使用制限するには，ＷＰＤデバイスを使用制限すればよいことからすれば，上記報告をもって，ＭＴＰ使用制御機能に対応したものは皆無であったとすることはできず，被告らの主張は，採用できない。

(ｳ) ③について

被告らは，経済産業分野ガイドラインにおいて，本件漏えい当時には，ＭＴＰ対応スマートフォンに対して何らかの対策を講じるべきとの具体的記載がされておらず，本件漏えい事件が発生した結果，そのような対策が追加されることになったことから，本件漏えい当時，ＭＴＰ対応スマートフォンに対して制御措置を採るべき注意義務はなかったとも主張する。そして，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で理事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で理事を務める己の意見書（乙３６「わが国におけるＰＣの外部記憶媒体とスマートフォンの歴史について」）には，本件漏えいは，それが発生する以前には一般に認識されていなかったセキュリティの脆弱性によって発生したもので，本件漏えい事件によって初めて，リムーバブルメディアとしての携帯電話（スマートフォンを含む）が外部記録媒体として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，ユーザーである被告シンフォームが予見することは不可能であった旨が記載されているほか，情報セキュリティの専門家等の記事（乙４０

・４１）にもその旨の記載がされている。

しかし，経済産業分野ガイドライン等の記載内容が直ちに被告らの注意義務の存否の判断を基礎づけるものではないことは，被告らも認めるとおりである。本件漏えいの時点における状況，とりわけ，被告シンフォーム自身が，大量の個人情報を扱い，現にＭＴＰ非対応スマートフォンへの書出しによる個人情報漏えいの危険を認識していたこと，ＭＴＰ対応スマートフォンが決して少なくない数になっていたこと，付与済みのアクセス権限の見直しが定期的に行われず（前提事実⑶イ），被告シンフォームが従業員の所属先を明確に把握していない（認定事実⑴エ）中で，業務委託先の従業員がスマートフォンを充電のため業務用ＰＣに接続していたことからすると，上記被告の主張やそれに沿う証拠を考慮しても，平成２６年当時において，丁のような者が存在しておかしくはなく，ＭＴＰ対応スマートフォンを業務用ＰＣのＵＳＢポートに接続することにより個人情報を不正に取得される可能性があることを認識し得たと認めるのが相当である。これらの被告らの主張は，採用できない。

㈡　④について

被告らは，被告らが一般ユーザーであることを強調するが，被告らは膨大な量の個人情報を扱っていたから，相応の予見，検討をすると考えられ，前記認定判断は決して被告らに不可能を強いるものとはいえない。

ウ　まとめ

以上によれば，被告らの主張を考慮しても，被告シンフォームは，本件漏えい当時，本件漏えいに用いられた方法であるＭＴＰ対応スマートフォンを業務用ＰＣのＵＳＢポートに接続する方法で，本件個人情報が不正に取得されるリスクがあることを予見し得たというべきである。

⑵　本件漏えいの回避義務

ア　双方の主張

少なくとも原告甲は，書出し制御等の回避措置をとる注意義務違反があった旨

主張する。

被告らは，被告シンフォームに，上記⑴のとおりの本件漏えいのリスクがあることについて予見可能性が認められる場合においても，原告甲の主張する各措置を講ずべき義務（結果回避義務）を負うものではないと主張する。

イ　基本的検討

丁は，金銭的に窮し，故意に，個人情報を取得し，名簿業者に売却した。それがすぐ露見したわけではないから，不正取得は，密かに行われたといえる。このような行為態様からみると，犯罪抑止効果を狙った監視カメラやアラートシステムの設定には効果がないと考えられる。また，ＵＳＢポートを塞ぐといった物理的な措置は，例えばＵＳＢデバイスであるマウスやキーボードさえも接続できなくなりかねず，制約として過度なものとなるから，現実的措置とはいえない。

そうすると，私物スマートフォンの持込み禁止の措置又は書出し制御措置（ＷＰＤデバイス使用制御措置）を採るべき義務の有無を検討するのが相当である。

ウ　私物スマートフォンの持込み禁止

⑺　前記⑴で認定したとおり，被告シンフォームは，本件漏えい当時，委託先の従業員が私物のＭＴＰ対応スマートフォンを被告シンフォーム多摩事業所の執務室内に持ち込み，業務用ＰＣのＵＳＢポートに接続することによって本件個人情報を含む大量の個人情報を取得するリスクがあることを予見しえたと認められる。これまで認めた事実によれば，被告シンフォーム多摩事業所の執務室内における私物のスマートフォンの持込み制限措置を採ることは，被告シンフォームにとって，コストも手間もかからない最も容易かつ効果の大きい不正防止対策であったと認められ，被告シンフォームが，丁が執務していた執務室内に，同人の私物のスマートフォン（本件スマートフォン）を持ち込むことを禁止する措置を採っていれば，本件漏えいを回避することができたといえる。

これまで認めた事実によれば，被告シンフォームは，本件漏えい当時，被告ベネッセから業務上の必要によって利用することを許されていた本件個人情報

を含む大量の個人情報について，業務委託先の従業員に業務用ＰＣを利用してアクセスすることを認める一方で，これらの従業員が業務用ＰＣに個人所有のスマートフォンを接続することが少なくなく，これを容認していたと推認できる。このような状況下では，被告シンフォームには，業務委託先の従業員がＭＴＰ対応スマートフォンを執務室内に持ち込んで上記個人情報に接することのないように，適切な措置を採るべき注意義務を負い，これを怠ったことについて過失があるというべきである。

(イ) 上記注意義務について具体的に述べると，以下のとおりである。

すなわち，丁の担当していた業務の内容は，本件サーバにアクセスして，本件データベースを扱って本件システムを開発するというものであり，機密性の高い個人情報に直接，頻繁に接する業務であり，そのような業務の内容からして，丁が本件システムを開発する業務と同時に，それ以外の通常の事務作業を並行して遂行する必要はなかったし，その業務を行うにおいて，私物のスマートフォンを使用する必要性が高いものであったことを認めるに足りる証拠もない。そうすると，丁は，基本的にはサーバルーム内での作業と遜色ない内容の業務を，執務室から本件サーバにアクセスして遂行していたものということができる。これは，外部記録媒体になり得るスマートフォンの持込みを制限する措置を採ることを検討するべき業務を執務室内で担当していたものといえ，執務室内にスマートフォンの持込みを禁止したとしても，その業務に支障を生じるものであったとはいえない。なお，被告シンフォームにおいて，本件漏えい当時，丁のように本件システム開発作業に従事させている者との関係でも，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があったというべきである。

(ウ) そして，以上のとおり，被告シンフォームにスマートフォン持込み禁止の注意義務を認めることは，以下のとおり，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リモ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ることにも沿うものといえる。

ａ　安全対策基準（上記①）について

安全対策基準（甲１３）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。この点，被告ベネッセは，安全対策基準が改正されたのが平成９年が最後であるところ，同年当時は未だスマートフォンが市場で流通していなかったから，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いえないと主張する。しかし，その時点では存在しない機器であっても，既に，セキュリティ保全のためには，搬出入物は必要な物に限定するという基準が置かれているのであるから，その趣旨に沿わない物は，将来的に開発される機器を含めて，その持込みを排除すべきとの趣旨には合理性が認められ，当時，スマートフォンが流通していないことをもって，安全対策基準の想定する対象物から除外すべきものと解することはできない。

ｂ　内部不正防止ガイドライン（上記②）について

内部不正防止ガイドライン（甲１８）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」については，「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，また，「重要情報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す。」との記載がされている。

この点，被告らは，内部不正防止ガイドラインは，「ＵＳＢメモリ等の記録媒体」と「スマートフォン等のモバイル機器」とを区別しており，「スマートフォン等のモバイル機器」については「サーバルーム」のみを対象としてその持込み・利用を制限する運用を推奨していたのであって，「サーバルーム」以外の執務室等は対象としていなかった旨主張する。

確かに，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，外部記録媒体をサーバ等の機器に直接接続することが可能であり，当該情報に直接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採る必要があると考えられるのに対し，通常の執務室のように，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必ずしも，同様の厳しい制限をすることまで要求されていないと解することも可能ではある。しかし，上記ガイドラインの趣旨は，重要情報に接触することができる業務に際しては，当該情報にアクセスすることによりそれが流出することを防止するという点にあることは明らかであり，そのために，個人所有の外部記録媒体を持ち込むことを禁じているのであるから，スマートフォン等のモバイル機器を持込み禁止とすべきかどうかについては，重要情報に接触する業務を行う場所であるか否かをもって判断されると解するのが合理的である。上記ガイドラインがサーバルームを記載するのは，重要情報に接触する機会が多いのがサーバルームであるから，それを例示的に取り上げているものと解され，サーバルーム以外の場所を対象外とする趣旨ではないと解される。

そうすると，内部不正防止ガイドラインもまた，重要情報に接触する業務を行う場所である場合には，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ことを認めないものではないというべきである。

ｃ　データセンターセキュリティガイドブック

なお，データセンターセキュリティガイドブック（甲９）では，共有区画

として，オフィスとサーバルームに区別され，サーバルームについては，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があるにとどまる。データセンターセキュリティガイドブックの記載は，場所により区分しているものと解される。しかし，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じるのであって，丁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考えられるから，上記の基準を作業場所の名称だけをもって単純に当てはめるのでは，セキュリティ保全を図る上記基準の趣旨を損なうものになることは否めない。したがって，データセンターセキュリティガイドブックの記載をもって，上記判断を左右することはできない。

エ　書出し制御措置及びＷＰＤデバイス使用制御措置について

原告甲の注意義務違反の主張は選択的であるから，持ち込み禁止以外の義務違反については検討する必要がないといえるが，被告シンフォームにおいて，他の結果回避措置を採ることで義務違反を免れることもできる関係にあるから，書出し制御措置を講じる義務を負っていたかについても検討する。

㈠　前記(1)で判断したとおり，被告シンフォームにおいては，本件漏えい当時，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を認識し得たのであるから，仮に，執務室内への私物スマートフォンの持込み禁止措置を行わないのであれば，情報漏えいを防ぐのに実効性が高く，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もあった情報の書出し制御措置又はＷＰＤデバイス使用制御措置を採るべき義務があったと解される。

確かに，被告らが本件漏えい当時使用していた本件セキュリティソフトには，ＭＴＰ対応スマートフォン（ＷＰＤデバイス）への書出し制御機能が備わっていなかったことが認められるが，ＷＰＤ使用制御機能は被告らが使用していた当時のバージョンの本件セキュリティソフトにも搭載されていたことが認められるのであるから，上記対策を採ることに特段の支障はなかったというべきである。

(イ) そうであるのに，被告シンフォームは，本件スマートフォンを含むＭＴＰ対応の他の種々のＷＰＤデバイスについては，これを接続して使用することが可能な状態にしており，それらを外部記録媒体として使うことによって，情報を書き出すことが可能な状態にしていたことが認められ，このことを調査確認によって容易に認識しえたにもかかわらず，上記対策をとることを怠っていたことが認められる。

(ウ) この点，被告らは，本件漏えい当時，①ＭＴＰ対応スマートフォンを含むスマートフォンに対する書出し制御措置を採るべきと明示していたガイドライン等はなかった，②被告シンフォームや被告ベネッセの情報セキュリティ対策は高度なものであり，他社の情報セキュリティ対策と比較しても，十分なものであったと主張する。

しかし，被告らは，本件個人情報を含む大量の個人情報を扱っていた。前記(1)で認定したとおり，本件漏えい当時，ＭＴＰ対応スマートフォンによる情報漏えいの危険性を予見でき，これを回避するための書出し制御措置又はＷＰＤデバイス使用制御措置を採ることができたものと認められるのであるから，ガイドライン等に記載がなかったことや同様の措置を採っている企業や法人が少なかったとしても，前記判断が左右されるものではない。

確かに，本件セキュリティソフトには，ＭＴＰ対応スマートフォンへの書出しを制御することができる機能は備わっていなかったから，書出しを制御するためには，ＷＰＤデバイスの使用自体を制御することにならざるを得ず，した

がって，デジカメやオーディオプレーヤーといったＷＰＤデバイスは総じて使用することができなくなることになる。しかし，被告シンフォームにおいて，本件システム開発等の業務を遂行するにつき，丁が使用する業務用ＰＣにボイスレコーダーやデジタルカメラ，さらにはスマートフォンといったＷＰＤデバイスを使用することができなくすることによって，その業務遂行が行えなくなるなどの弊害が生じるということの主張立証はない。

現実にも，本件漏えい後の遅くとも平成２６年９月１７日以降，被告シンフォームは，対応策として，ＷＰＤデバイスその他の書出し機能を持つ可能性のある全ての外部デバイスの使用を制御する措置を採り，その後もこれを解除したことを認めるに足りる証拠はないから，本件システム開発業務において，業務用ＰＣにＷＰＤデバイスを接続してデータを通信する必要性があったものとは認められず，そうであれば，本件漏えい以前からこれと同じ対策を講ずることができたということができる。そして，仮に，本件システム開発業務を行う従業員において，特定の機器（ＷＰＤデバイス）を接続する必要性が生じた場合には，その都度，被告シンフォームの承認の下に当該機器についてだけ上記制御措置を解除して接続することも可能であったから，上記の単なる不便さが生じることをもって，ＷＰＤデバイスに対する使用制御措置を採らなかったことを正当化し得る理由とはならない。

なお，被告シンフォームにおいて，ＷＰＤデバイスに対する使用制御措置を採ることが困難な事情が認められるのであれば，それに代えて，上記のとおり，本件スマートフォンを執務室内に持ち込むことを禁止する措置を採るべきであったと認められる。

したがって，被告シンフォームは，本件漏えい当時，ＭＴＰ対応スマートフォンを含むＷＰＤデバイスに対する使用制御措置（書出し制御措置を含む。）を採っていなかったことについて注意義務違反（過失）があったといわざるを得ない。

⑶　まとめ

以上のとおり，本件漏えい当時，被告シンフォームは，本件漏えいを予見できたのに，ＭＴＰ対応スマートフォンの持込みを禁止すべき注意義務及びこれに対するＷＰＤデバイス使用制御措置（書出し制御措置を含む。）を採るべき注意義務に違反したため，丁の故意による本件漏えいを防止できなかったといえる。被告シンフォームは，原告甲に対し，不法行為による損害賠償責任を負う。

４　争点⑵（本件漏えいについての被告ベネッセの過失の有無）について

⑴　本件漏えいの予見可能性

前記３⑴において，被告シンフォームについて記載したところと同様に，被告ベネッセにおいても，本件漏えい当時，本件漏えいの方法で個人情報を不正に取得できる可能性があることを予見できたと認めるのが相当である。

⑵　回避可能性及び回避（注意）義務違反について

ア　委託先の選任及び監督以外に関する注意義務違反

原告甲が主張する個人情報の利用・管理に責任を持つ部門の設置義務については，このような組織があったとしても，当該組織が本件漏えいの発生を回避するためにどのような具体的対応をすることができたのかは主張としても不明といわざるを得ず，当該組織を設置しただけで，本件漏えいを回避できたとは認められない。また，被告シンフォームに対するのと同様のスマートフォン持込み禁止等に関する種々の注意義務については，本件漏えい当時，被告シンフォームが被告ベネッセの１００％子会社であったこともあるグループ会社というだけでは，被告シンフォームの過失を被告ベネッセの過失と同視することはできないから，これらの点において被告ベネッセの過失をいう原告甲の主張は理由がない。

以下，委託先の選任及び監督に関する注意義務違反があるか否かを検討する。

イ　委託先の選任及び監督に関する注意義務違反

㈠　検討

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，委耗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，証拠（甲１０，１９）によれば，経済産業分野ガイドライン（甲１０）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扱い状況を把握することが含まれる旨の記載があり，ＪＩＳＱ１５００１（甲１９）には，「3．4．3．4　委託先の監督」において，文書審査の項目として「委託先選定基準を定める手順及び見直しの手順を定めていること」とし，現地審査の項目として①「定めた手順に従い，委託先選定基準を確立させていること」，②「必要に応じて委託先選定基準の見直しを実施していること」とし，現地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」などの記載があると認められる。

また，これまで認めた事実によれば，被告ベネッセは，本件個人情報を含む大量の個人情報を顧客から提供を受けて管理し，これを個人情報提供者の了解の下に，営業目的等に使用していたところ，本件システム開発等の業務に必要であるとして，業務委託先である被告シンフォーム及びその再委託先等の従業員が委託業務に必要な範囲でこれらの個人情報に接することを認めていた。被告ベネッセが，業務委託先の従業員に上記個人情報へのアクセスを認めることについて個人情報提供者から明示の承諾を得ていたことを認めるに足りる証拠はない。

以上によれば，被告ベネッセには，本件漏えい当時，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認めるのが相当である。しかし，前記(1)記載のとおり，被告ベネッセは，本件漏えい当

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が，弁論の全趣旨によれば，それにもかかわらず，被告シンフォームに対し，本件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出し制御機能等を備えているか否か，被告シンフォームの業務委託先の従業員が，被告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が容易に推認される。これらについて適切に指導監督を行っていれば，本件セキュリティソフトにおけるＭＴＰ対応スマートフォン（ＷＰＤデバイス）に対する使用制御措置を採るように指示することができ，それが困難であったとしても，被告シンフォームに対し，業務委託先の従業員が本件個人情報を含む大量の個人情報に接することができる執務室内に，個人のスマートフォンを持ち込むことを禁止するよう指示することができたというべきで，このような指導監督を行うことについて，被告ベネッセに過度の負担が生じるということはなかったと認められる。

そうすると，被告ベネッセには，本件漏えい当時，被告シンフォームにおける被告ベネッセの有する個人情報の管理につき，本件セキュリティソフトのＷＰＤデバイス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いうべきであり，それにもかかわらず，被告ベネッセは，本件漏えい当時，これらについて指示することなく放置していた結果，本件漏えいを回避することができなかったのであるから，上記注意義務に違反したといわざるを得ない。なお，経済産業大臣作成の平成２６年９月２６日付け「個人情報の保護に関する法律第３４条第１項の規定に基づく勧告について」と題する書面においても，被告シンフォームにおいて，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，被告ベネッセは，被告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条に反すると指摘されている（甲２３の２）。

(イ) 被告ベネッセの主張の検討

被告ベネッセは，本件漏えい当時，経済産業分野ガイドラインや情報セキュリティ対策の一般的な水準からしても，明らかに高度な水準で被告シンフォームに対する委託先監督を実施していたなどと主張する。

しかし，被告ベネッセは，大量の個人情報の運用管理を被告シンフォームに委託して，被告ベネッセと直接の契約関係のない被告シンフォームの業務委託先の従業員が本件個人情報を含む大量の個人情報に接することを容認していたにもかかわらず，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て，被告シンフォームに対し，前記認定説示の監督をしなかったのであるから，被告ベネッセの上記主張は理由がない。このことは，被告ベネッセがプライバシーマークを取得していたことを考慮しても同様である。

むしろ，被告ベネッセは，本件漏えい当時，ＭＴＰ対応スマートフォンによる情報漏えいの危険性を予見でき，被告シンフォームに対する監督によって本件漏えいを回避することができたと認められるのであるから，ガイドライン等に具体的に記載がなかったことや同様の措置を採っている会社が少なかったとしても，前記判断が左右されるものではない。

(3) まとめ

以上のとおり，被告ベネッセは，個人情報提供者から提供を受けた個人情報を適切に管理すべき立場にあり，本件漏えいのリスクを予見できたのに，当該個人情報の利用を認めた被告シンフォームに対する適切な監督義務に違反した結果，丁による本件漏えいを防止できなかったと認められるから，原告甲に対し，これによって生じた損害について不法行為責任（民法７０９条）を負うものと認められる。

５　被告らに関する損害賠償責任の成否のまとめ

⑴　原告甲関係

被告ベネッセと被告シンフォームの不法行為（及び丁の本件漏えいによる不法行為）は，被告ベネッセが保有し，その管理を被告シンフォームに委託して管理させていた本件個人情報の漏えい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，共同不法行為に当たると認められる（民法７１９条１項前段）。

また，共同不法行為と使用者責任とで損害が異なるともいえない。

そうである以上，被告シンフォームは，丁の使用者との間の委託関係の詳細を明らかにしないが，原告甲が選択的に主張する被告ベネッセの被告シンフォームに対する使用者責任（争点⑶イ）並びに丁の本件漏えい行為を不法行為としてそれに対する被告シンフォーム及び被告ベネッセそれぞれの使用者責任（争点⑶アイ）を問う主張については，いずれも判断する必要がない。

⑵　原告乙及び原告丙関係

原告乙及び原告丙については，原告甲の主張するような具体的な注意義務違反等についての主張がされていない。前記第２の３冒頭のとおり，原告らのうち，原告乙は，平成２８年１月２０日の本件第６回弁論準備手続期日に出頭した後は，本件の口頭弁論期日にも弁論準備手続期日にも出頭しておらず，原告乙及び原告丙の主張は，それまでのものに限られる。原告乙及び原告丙は，被告らの不法行為責任はもちろん，原告甲について検討しなかった使用者責任についても，抽象的な主張をするにとどまる。原告乙及び原告丙に対する関係では，損害について判断するまでもなく，被告らの責任を認めることはできない。

６　争点⑷（原告甲に生じた損害の有無及び数額）について

⑴　精神的損害

ア　判断枠組み

前記２⑴で判断したとおり，本件個人情報は，原告甲のプライバシーに関する情報として法的保護の対象となるから，上記認定事実によれば，本件漏えいによって，原告甲はそのプライバシーを違法に侵害されたと認められる。

そして，個人情報が外部に漏えいしてプライバシーが侵害された場合に，当該被漏えい者が精神的苦痛を被ったか否か及び被った精神的損害を慰謝するに相当な額を検討するに当たっては，流出した個人情報の内容，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，本件において顕れた事情を総合的に考慮して判断すべきである。

イ　個人情報の内容

本件で流出した個人情報の内容は，前記認定のとおり，原告甲の漢字氏名，フリガナ，住所，電話番号，原告丙の漢字氏名，フリガナ，生年月日，性別である。原告丙の漢字氏名，フリガナ，生年月日，性別は，原告甲の個人情報そのものではないとしても，原告甲の家族関係を表す情報といえることから，本件個人情報は，いずれも原告甲の個人情報であると認められる（前記２(1)）。

次に，これらの情報のうち，原告甲の漢字氏名，フリガナ，住所及び電話番号は，いずれも原告甲の個人識別情報と連絡先であり，自らが生活する領域においては，必要に応じて第三者に開示される性質の情報であって，こうした情報だけでは，個人の職業等の社会的地位，資産等の経済的な情報や思想信条等の情報と一体となっている情報に比べると，一般的に「自己が欲しない他者にはみだりに開示されたくない」私的領域の情報としての性質は低いといえる。もっとも，こうした情報も，今日のように，情報ネットワークが多様化，高度化し，容易に入手可能なさまざまな情報を組み合わせることによって趣味嗜好や思想等まで把握されかねない危険性のあることが危慎されていることにも鑑みると，本件個人情報は，個人特定の基本となるベース情報として機能し，それを基に情報集積がされかねないものとしては重要な価値を持つものと評価すべきである。また，子である原告丙の漢字氏名，フリガナ，生年月日及び性別については，これらも日常的に開示されることが多いものであるとはいえ，家族関係が一定程度明らかになる情報（原告甲の原告丙との続柄が開示されたに等しいことは前記認定のとおりである。）や教育に関心が高いという属性が含まれており，前者に比してより私

的領域性の高い情報ということができる。

ウ　流出した範囲，実害の有無等

本件個人情報は，情報流出元が被告ベネッセという教育関係の会社であったことや原告丙の年齢等から今後の学業生活等に関する支出が見込まれる顧客情報として，それらに関係する業者からは価値のある情報として有望視されることは避けられないものといえる。原告甲が，それら業者等からの広告，販売活動を受け，それに煩わしさや不快を感じる機会が増大することが予想される。なお，本件においては，原告甲が転居し（弁論の全趣旨），住所及び電話番号を変更したため，そのような機会は減少したと推認されるが，それは原告甲の行動の結果であり，そのような行動を起こす前に原告甲が被った精神的苦痛は，そのような行動を起こさなかった者の場合と変わるものではない。

もっとも，原告甲においても，現時点においては，いわゆる「ハレノヒ事件」のような被害に遭うかもしれないと主張するだけで（原告ら準備書面(17)），現実にそのような被害に遭ったという主張はないし，ダイレクトメールが増大するなどして，原告甲に何らかの実害が生じたという主張，立証もない。

しかし，その流出範囲については，丁が相当期間にわたって本件漏えいを行っていたこと（認定事実(2)ウ）などから，被告ベネッセにおいても確認できない状況にあることが容易に推認され（甲２７，乙１７），流出した情報の全てを回収して抹消させることは不可能な状況となっているといわざるを得ない。被告ベネッセに個人情報を開示した顧客の一人である原告甲にとって，原告甲の承諾もないままに丁によって故意かつ営利目的を持って本件個人情報が流出したこと自体が精神的苦痛を生じさせるものである上，その流出した先の外縁が不明であることは原告甲の不安感を増幅させるものであって，このような事態は，一般人の感受性を基準にしても，その私生活上の平穏を害する態様の（すなわち社会生活上の受忍限度を超える違法な）侵害行為であるというべきである。

この点，被告ベネッセは，本件漏えいでは，本件個人情報が流出しただけであ

って，抽象的な不安感にとどまるから，損害賠償請求の対象となり得る損害に該当しないなどと主張する。しかし，本件個人情報を利用する他人の範囲を原告甲が自らコントロールできない事態が生じていること自体が具体的な損害であり，原告甲において予め本件個人情報が名簿業者に転々流通することを許容もしていないのであるから，上記のような現状にあること自体をもって損害と認められるべきである。

エ　被告ら側の対応

他方，証拠（甲８，３１，３９）及び弁論の全趣旨によれば，被告らの持株会社であるベネッセホールディングスが，本件漏えいの発覚後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，原告甲を含む情報が漏えいしたと思われる顧客に対し，お詫びの文書を送付するとともに，顧客の選択に応じて５００円相当の金券を配布するなどしたことが認められる。

オ　慰謝料額の判断

そうすると，原告甲のプライバシー権の侵害態様，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のほか，本件個人情報が原告甲の子である原告丙の個人情報として被告ベネッセに対して提供されたものであることなど，本件に顕れた一切の事情を考慮すれば，原告甲の被った精神的損害を慰謝するには１０００円を支払うべきものと認めるのが相当である。

⑵　財産的損害

原告甲は，平成２６年７月１２日付けで被告ベネッセ宛に漏えいした項目を確認するための内容証明郵便を送付し，その送料として１２６０円を要し，また，被告ベネッセからの「お詫び」として５００円相当の金券を用意する旨の案内に対する異議申立てを簡易書留で送付し，その送料として４３０円を要したことから，これらの合計１６９０円も原告甲の損害として認められるべき旨主張する。

前記認定説示に加え，証拠（甲３，４，８）によれば，原告甲が主張するとおりの経費が支出されたことが認められる。

そして，このような支出は，本件漏えいがなければ発生しなかったといえるほか，被告らにとって予想可能な範囲であるといえる。

そうすると，上記１６９０円の賠償義務も認めるのが相当である。

⑶　まとめ

原告甲の人格権の侵害により生じた損害は，１０００円＋１６９０円＝２６９０円となる。

第４　結論

以上によれば，原告甲の請求は，２６９０円及び対応する遅延損害金の支払を求める限度で理由があるから，その限度で認容し，その余の原告甲の請求並びに原告乙及び原告丙の各請求はいずれも理由がないから棄却するのが相当である。

京都地方裁判所第２民事部

裁判長裁判官　　久　留　島　　群　　一

裁判官　　鳥　　飼　　晃　　嗣

裁判官　　浦　恩　城　　泰　　史