主　　文

1　原判決を次のとおり変更する。

(1)　被控訴人は，控訴人に対し，１０００円及びこれに対する平成２６年１１月２８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)　控訴人のその余の請求を棄却する。

2　訴訟費用は，差戻し前一審，差戻し前控訴審，上告審（上告提起事件を除く。）及び差戻し後の控訴審（当審）を通じ，これを１００分し，その１を被控訴人の負担とし，その余を控訴人の負担とする。

3　この判決は，第１項(1)に限り，仮に執行することができる。

事　実　及　び　理　由

第１　控訴の趣旨

1　原判決を取り消す。

2　被控訴人は，控訴人に対し，１０万円及びこれに対する平成２６年１１月２８日から支払済みまで年５分の割合による金員を支払え。

第２　事案の概要

1　事案の骨子及び訴訟経緯

(1)　事案の骨子

本件は，控訴人が，被控訴人において管理をしていた控訴人の個人情報を含む顧客らの個人情報を，被控訴人から委託を受けて個人情報を分析するシステム（以下「本件システム」という。）の開発をしていた株式会社Ａの委託先の従業員であるＢが外部に漏えいさせたことから，精神的苦痛を被ったと主張して，被控訴人に対し，選択的に，①被控訴人には，控訴人の個人情報の管理に注意義務違反があったとして被控訴人の不法行為（民法７０９条）に基づき，②また，被控訴人には，株式会社Ａ（株式会社Ａには，(ア)株式会社Ａ自体に個人情報の管理に注意義務違反があった（民法７０９条），あるいは(イ)Ｂによる漏えい行為が株式会社Ａの事業の執行につきなされたとして

その使用者責任があった（民法７１５条１項本文）。）の選任監督に係る注意義務違反があったとして株式会社Ａの上記㋐，㋑の不法行為との共同不法行為（民法７１９条１項前段）に基づき，③さらに，株式会社Ａは被控訴人の被用者であり，株式会社Ａの上記②㋐，㋑の不法行為は被控訴人の事業の執行につきなされたとして，使用者責任に基づき（民法７１５条１項本文），慰謝料１０万円及び不法行為後の日である平成２６年１１月２８日（訴状送達日の翌日）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た事案である。

⑵　訴訟の経緯

ア　本件の差戻し前の１審（神戸地方裁判所姫路支部平成２７年㋫第４２４号）は，被控訴人の管理する控訴人の氏名が漏えいしたことのみを争いのない事実として認定した上で，これが被控訴人の過失によるものであることを基礎付けるに足りる具体的事情の主張立証がないとして，控訴人の請求を棄却した。

イ　これに対し，控訴人が控訴したところ，差戻し前の控訴審（大阪高等裁判所平成２８年㋬第３７号）は，被控訴人の管理する控訴人の子であるＣの氏名，性別，生年月日，郵便番号，住所，電話番号，保護者名（控訴人の氏名）が漏えいしたことを認定した上で，これをもって，控訴人の氏名・郵便番号，住所，電話番号及びその家族である者の氏名，性別，生年月日という控訴人自身の個人情報が漏えいしたものということができるとしたうえで，上記の控訴人の個人情報の漏えいは，通常人の一般的な感覚に照らして，不快感のみならず，不安を抱くことがあるものであると認めながら，そのような不快感等を抱いただけでは，これを被侵害利益として，直ちに損害賠償を求めることはできないものと解されるとして，上記の不快感等を超える損害を被ったことについての主張立証がないことを理由に控訴を棄却した。

ウ　控訴人が，これに対して上告受理を申し立てたところ，最高裁は，これを受理した上，本件の事実関係の下では，本件漏えいによって控訴人はそのプライバシーを侵害されたといえるところ，原審は，上記のプライバシーの侵害による控訴人の精神的損害の有無及びその程度等について十分に審理することなく，不快感等を超える損害の発生についての主張立証がされていないということのみから直ちに控訴人の請求を棄却すべきものとしたものであり，そのような原審の判断には，不法行為における損害に関する法令の解釈適用を誤った結果，上記の点について審理を尽くさなかった違法があるとして，原判決を破棄し，被控訴人の過失の有無並びに控訴人の精神的損害の有無及びその程度等について更に審理させるために本件を当審に差し戻した。

2　前提事実（当事者間に争いのない事実並びに掲記の証拠及び弁論の全趣旨により容易に認定できる事実）

⑴　当事者

ア　控訴人は，被控訴人の講座を受講したことがある未成年者・Ｃの保護者（父親）である。

イ　被控訴人は，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「進研ゼミ」や「こどもちゃれんじ」などを展開し，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，子供の氏名，性別，生年月日，住所，電話番号，保護者名などを，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　控訴人は，Ｃが被控訴人の講座を受講するに際し，本件個人情報を含むＣの個人情報を被控訴人に提供し，被控訴人は，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。（弁論の全趣旨）

エ　株式会社Ａは，被控訴人のいわゆるグループ会社（平成２６年６月当時

は被控訴人のいわゆる１００％子会社）で，被控訴人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。

オ　被控訴人は，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株式会社Ａに委託した。

カ　Ｂは，同年１月に株式会社Ａの業務委託先の会社の従業員（システムエンジニア）となり，同年４月頃から，同社従業員として，株式会社Ａ東京支社多摩事業所（以下「株式会社Ａ多摩事業所」という。）において，被控訴人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，控訴人の本件個人情報を含む被控訴人の受講者の個人情報の集まり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。）が記録された被控訴人のサーバコンピュータ（以下「本件サーバ」という。）に株式会社Ａ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ＩＤ及びパスワード等（業務用アカウント等）を付与されていた。

⑵　本件漏えい

ア　Ｂは，平成２６年６月１７日及び同月２７日に，株式会社Ａ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，被控訴人が管理する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自己のスマートフォン（平成２４年１２月頃に発売されたモデルで，ＯＳは同年６月２７日に

リリースされた「Ａｎｄｒｏｉｄ４．１」を搭載しており（甲２０），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（甲９））に対応している。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。）。（甲１７，６８，８７）

イ　Ｂが漏えいした顧客情報のうちには，控訴人の子であるＣの氏名，性別，生年月日，郵便番号，住所，電話番号，保護者名（控訴人の氏名）及び控訴人とＣとの続柄（以下では，Ｃ及び控訴人の個人情報を併せて「本件個人情報」という。）が含まれていた。（甲１，２）

ウ　本件漏えいの発覚等

被控訴人は，同年６月下旬頃，顧客から，被控訴人に登録した個人情報が漏えいしているのではないかとの問い合わせが急増したことから，調査を行い，Ｂが本件漏えいをしたことを特定し，直ちに同年７月９日，被控訴人の持株会社である株式会社ベネッセホールディングス（以下「ベネッセホールディングス」という。）のＤ（役職名省略）が記者会見し，本件漏えい事故を公表し，その原因を徹底的に明らかにすると共に，被控訴人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１，２）

⑶　被控訴人による事後措置

ア　被控訴人は，平成２６年７月１０日，経済産業大臣から，個人情報保護法３２条に基づく報告を命じられた。（甲３）

イ　被控訴人は，同月１１日以降，お詫びと本件漏えいの対策状況を新聞広告によって公表した。

ウ　被控訴人は，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」（被控訴人が本件漏えいを受けて子らへ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１８の３）。控訴人（C）は，上記５００円の金券を得る方法を選択しなかった（甲４）。

エ　D（役職名省略）は，同月１５日，その諮問機関として，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（乙３の２）。

本件調査委員会は，事故調査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，被控訴人は，同月１７日，最終報告書を経済産業省に報告するとともに，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６）。

上記事故調査報告書には，「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６）。

㋐　アラートシステム

クライアント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株式会社Ａ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，Ｂ

による不正行為が行われた当時，クライアント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。

㈠　クライアントＰＣ上のデータのスマートフォンへの書出し制御設定

株式会社Ａでは，クライアント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が採用されていたが，当該システム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。

㈡　アクセス権限の管理

株式会社Ａ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。

㈢　データベース内の情報管理

株式会社Ａ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

控訴人は，本件訴訟において，選択的に，被控訴人の不法行為に基づく損害賠償請求（民法７０９条），被控訴人と株式会社Ａとの間の共同不法行為に基づく損害賠償請求（民法７１９条），被控訴人の株式会社Ａを被用者とする使用者責任に基づく損害賠償請求（民法７１５条。株式会社Ａの不法行為責任ないしＢを被用者とする使用者責任を前提とする。）を理由として，被控訴人に対して損害賠償を請求している。

⑴　争点⑴（民法７１９条１項，同法７１５条に基づく各請求）

本件漏えいについて株式会社Ａの過失の有無

【控訴人の主張】

ア　Ｂによる本件漏えいは，外部と繋がるインターネット環境を利用し，被控訴人の情報セキュリティを掻い潜って個人情報を盗み出したという態様のものではなく，もともと被控訴人から大量の個人情報についてアクセス権限を与えられていた者が，監視のない中で，自由に持ち込んだ個人所有のスマートフォンを，ＵＳＢケーブルを使用して株式会社Ａが管理する業務用ＰＣと繋げ，被控訴人が管理する個人情報をダウンロードしたうえ，アラートシステムが対応しない状況下で盗み出したという単純な手法により実行されたものであり，株式会社Ａ及び被控訴人の過失は明らかである。

イ　本件漏えいの予見可能性

㈠　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保存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。

①　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１６）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」と記載されていた。

②　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ー要求事項（ＪＩＳ　Ｑ　１５００１：２００６）」（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「ＪＩＳ　Ｑ　１５００１：２００６をベースと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２１）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掲げられていた。

③　「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８，乙１１）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。

④　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１４）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。

⑤　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７）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をセキュリティ対策として挙げられていた。

㈠　また，株式会社Ａ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出し制御が実施されている旨を周知させており，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　Ｂ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）である「ｉＯＳ」及び「Ａｎｄｒｏｉｄ」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に対応したものであるが，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，代表的なセキュリティソフトがＷＰＤ（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，株式会社Ａ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。

ウ　株式会社Ａ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（各主張はいずれも選択的）。

㈠　私物スマートフォンの持込みに係る注意義務違反

株式会社Ａ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，上記イ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上げられている。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，上記イ㈡のとおり，株式会社Ａ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，株式会社Ａ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ものである。

さらに，株式会社Ａ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顧客情報にアクセスすることが可能な状況にあったものであり，そうであれば，株式会社Ａ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，株式会社Ａ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，株式会社Ａ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，株式会社Ａ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）に係る注意義務違反

上記イ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，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，株式会社Ａ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，株式会社Ａ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，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。また，自治体でも，既に平成２０年には，千葉県袖ヶ浦市でＵＳＢポートを物理的に塞塞する方法が検討されていた。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，株式会社Ａ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執らず，また，業務用ＰＣに充電のために個人のスマートフォン

などを接続することが日常的に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。

㈢　情報書出し制御措置・デバイス使用制御措置に係る注意義務違反

上記イ㈠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書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，上記イ㈡のとおり，株式会社Ａ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。

そして，Ｂ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ところ，上記イ㈢のとおり，代表的な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，ＷＰＤ（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，ｉＯＳ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，ＷＰＤ（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ところ，代表的な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，株式会社Ａ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，株式会社Ａ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，株式会社ＡがＭＴＰデバイスを制御の対象から外していたうえ，ＭＴＰによる通信について，書き出し制御の対象となっていない同ソフトウェアを使用し続けていたために，Ｂ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，株式会社Ａには，本件漏えい当時，業務用ＰＣにＷＰＤ（ＭＴＰ）使用制限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，情報の書出し制御措置あるいはＭＴＰ使用制限措置を採るべき注意義務があったにもかかわらず，通信方式がＭＴＰである機器への情報書出し制御措置機能のない本件セキュリティソフトを使用し続け，かつ，同セキュリティソフトに備わっていたＷＰＤ（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。

㈡　アラートシステム設定に係る注意義務違反

上記イ㈠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，前記イ㈡で述べたとおり，株式会社Ａ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。

株式会社Ａ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高かったのであるから，業務用ＰＣから本件データベースにアクセスされ，それが通常業務における以上の通信量と認められた場合，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，株式会社Ａは，既存の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。

㈎　監視カメラ等の画像による監視義務違反

上記イ㈎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，上記イ㈑のとおり，株式会社Ａ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。

株式会社Ａ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，株式会社A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。

【被控訴人の主張】

ア　株式会社A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ことや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ことは，当時の状況を顕現している。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識されたのである。

株式会社Aにおいても，本件漏えい以前に，業務用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もなければ，充電のため業務用ＰＣに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

ができる等の報告等がされたことも一切なく，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，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かかる注意義務違反について

㈠　各基準について

①　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，株式会社Ａ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」は「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なされた平成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，控訴人が，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。

②　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，控訴人が，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。

③　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としてみるには不適当な性質のものであり，被控訴人の注意義務の根拠たり得ない。また，控訴人が，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。

④　その他のガイドライン等

上記以外に，控訴人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ものである。

㈠　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のみならず，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い。

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接続禁止措置にかかる注意義務違反について

㈠　各基準について

①　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ところ，Ｂの使用する業務用ＰＣはかかる端末ではなかった。

②　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のであるから，控訴人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。

③　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したガイドラインであるから，法規範性を有するものではない。

(イ)　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のみならず，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，かかる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ではかかるセキュリティ対策をとっていなかったのであるから，業務用ＰＣに対するＵＳＢ接続禁止措置は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デバイス（株式会社Ａでは，一定の要件のもとに許可されたＵＳＢメモリ）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　書出し制御措置にかかる注意義務違反について

(ア)　各基準について

①　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，株式会社Ａ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。

② 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。

㈠ 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，株式会社Ａ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，株式会社Ａ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（株式会社Ａ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。），株式会社Ａの執務室内のクライアント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ものであり，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な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にスマートフォンを接続して書き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，この結果とし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ことから，本件漏えい当時，ＭＴＰ対応の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いものであることを知りえなかった。この点について控訴人は，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１０）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いなかったもので，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を生ずるものではない。なお，株式会社Ａ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かかる注意義務違反について

㈠　各基準について

①　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，株式会社Ａの注意義務の根拠たりえない。

②　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，経済産業省が被控訴人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（株式会社Ａ）において，今回の不正書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。

㈡　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ないし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　監視カメラにかかる注意義務違反について

㈠　各基準について

①　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，株式会社Ａの注意義務の根拠たりえないし，控訴人が，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。

②　データセンターセキュリティガイドブック

データ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ており，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) 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，かかる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，株式会社Ａ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　以上のとおりであるから，株式会社Ａ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。

⑵　争点⑵（民法７１９条１項，同法７０９条の各請求）

本件漏えいについて被控訴人の過失の有無

【控訴人の主張】

前記⑴の「控訴人の主張」に記載したと同様の理由で，被控訴人には本件漏えいによって控訴人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⑴の控訴人の主張イに同じ。

イ　被控訴人には，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かかる注意義務違反

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，「⑵　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ている。

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，被控訴人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，被控訴人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株式会社Ａに委ね，株式会社Ａが同業務の一部をさらに第三者に委託し，被控訴人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，被控訴人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，被控訴人には，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，被控訴人は，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，個人情報課など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，株式会社Ａに対する適切な監督を妨げ，株式会社Ａ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。

⑷　私物スマートフォンの持込み等に係る注意義務違反

被控訴人は，本件システムの開発・運用を株式会社Ａに委託していたものの，元々が株式会社Ａ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，株式会社Ａの役員に被控訴人の役員が就任していた状況からすると，被控訴人は，実質的には株式会社Ａを自社の一部門と同様の状態で事業を行っていたものであるから，株式会社Ａ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，被控訴人自身が，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。

㈢　委託先選任及び監督にかかる注意義務違反

被控訴人は，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株式会社Ａ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，被控訴人は，個人情報保護法上，株式会社Ａ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，被控訴人は，株式会社Ａから契約内容の遵守について定期的に報告を受けたり，株式会社Ａ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，「審査の着眼点」として，「委託先を選定する基準として，該当する業務については少なくとも自社と同等以上の個人情報保護の水準にあることを客観的に確認できること，選定基準は具体的で運用なものであること」等を例示していた。

これに，前記のとおり，被控訴人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，被控訴人は，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，被控訴人は，株式会社Ａ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かかる体制であることを把握せずに委託先に株式会社Ａを選任した。

また，被控訴人は，株式会社Ａ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，株式会社Ａによる被控訴人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，被控訴人は，株式会社Ａ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，被控訴人は，以上のような株式会社Ａ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，さらに株式会社Ａ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Ｂ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，被控訴人には，本件漏えいについて委託先の選任及び監督に係る過失があった。

ウ　以上によれば，本件システム開発は，被控訴人と株式会社Ａ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，被控訴人は，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，被控訴人が保有・管理していた個人情報を株式会社Ａ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，被控訴人と株式会社Ａ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）。

【被控訴人の主張】

被控訴人には，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⑴の被控訴人の主張イに同じ。

イ　個人情報の利用・管理に責任を持つ部門設置にかかる注意義務違反について

被控訴人は，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のであるから，控訴人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，それは個人情報取扱業者に対して義務を課す行政法規であって，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。）し，本件漏えいとの間に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にかか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。控訴人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，株式会社Ａが私物スマートフォンの持込みに係る注意義務を負うとしても，被控訴人が同様に注意義務を負うということはできない。

エ　委託先選任及び監督にかかる注意義務違反について

㈠　そもそも，株式会社Ａにおいて，控訴人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係る注意義務，ＵＳＢ接続禁止に係る注意義務，書出し制御に係る注意義務，アラートシステム設定に係る注意義務，監視カメラによる監視に係る注意義務）は存在しなかったから，株式会社Ａがかかる措置を採っていなかったからといって，被控訴人に委託元としての選任監督の注意義務違反はない。

㈡　株式会社Ａ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，社会的に高い情報セキュリティ管理レベルを期待される，製造，流通，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，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，株式会社Ａ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，株式会社Ａは，当時の経済産業分野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，被控訴人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。

㈢　被控訴人は，本件漏えい当時，当時の経済産業分野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セキュリティ対策を採っていた委託先である株式会社Ａに対して，必要な監督を実施していた。

オ　以上のとおりであるから，被控訴人には，本件漏えいについて予見可能性がなかったもので，これを回避するについての注意義務（株式会社Ａ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　控訴人による被控訴人の不法行為（民法７０９条）及び株式会社Ａ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　株式会社Ａは，Ｂ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）

【控訴人の主張】

㈠　株式会社Ａ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，Ｂ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，株式会社ＡとＢとの間に直接の雇用関係はないが，Ｂは，システムエンジニアとして株式会社Ａに派遣され，株式会社Ａ多摩事業所で被控訴人の情報システムの開発等に関する業務に従事し，日常的に株式会社Ａの社員から指示を受けていた。また，株式会社Ａは，Ｂに対し，株式会社Ａ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，株式会社Ａは，本件システム開発に関する事業について，Ｂ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

Ｂによる本件漏えいは，被控訴人から株式会社Ａが委託を受けた本件システム開発等の業務を，株式会社Ａ多摩事業所においてＢが行っている際にされたものであるが，Ｂ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ものであるから，本件漏えいは，株式会社Ａの「事業の執行」に該当する。

㈡　したがって，株式会社Ａは，Ｂによる本件漏えいについて使用者責任を負う。なお，選任監督上の相当の注意をしていたとの被控訴人の主張は争う。

【被控訴人の主張】

㈠　株式会社Ａの使用者性について

株式会社Ａ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，株式会社Ａ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，Ｂ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がこれを行っていたものであるから，株式会社Ａは，Ｂを実質的に指揮監督する関係にはなかった。

㈡　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。Ｂ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，株式会社Ａ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，控訴人は，Ｂ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，そもそも株式会社Ａの事業ではあり得ないし，Ｂの職務の範囲内であることもおよそ考えられない。

�given　選任監督上の相当の注意をしていたこと

本件において，株式会社Ａは，Ｂ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，Ｂ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，株式会社Ａは，同社とＢ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　被控訴人は，株式会社Ａの不法行為について使用者責任を負うか否か（争点⑶イ）

【控訴人の主張】

㈠　事業執行性

本件システムは，被控訴人の商品・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，被控訴人の「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

使用関係の有無を判断するにあたっては，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，被控訴人と株式会社Ａとの間の業務委託契約では，被控訴人が，被控訴人が行っている安全管理措置と同等の措置が株式会社Ａでも採られるように監督することや，株式会社Ａが受託業務を再委託する場合には，事前に被控訴人の承諾を求めることとしていた（甲１８の３：最終報告書１２頁）。また，被控訴人は，株式会社Ａ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。

また，被控訴人は，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（甲第１８号証の３：最終報告書３０頁）。被控訴人は，本件データベースの運用にあたり，開発中の本件システムの動作状況を確認し，株式会社Ａに対してミーティング等でシステムの障害や不具合の改善を指示していた。

さらに，被控訴人は，個人情報の保護要件が変更になった場合には，説明会を実施して株式会社Ａの幹部社員に説明を行うほか，ミスやトラブルが発生した場合には，その都度株式会社Ａのセキュリティの設定状況の確認を行っていた。

また，本件漏えい当時，株式会社Ａは，被控訴人の１００％子会社の関係にあったものであり，本件システム開発以前から，被控訴人の指示のもと，被控訴人の事業に関するシステムの開発・運用を担当していた。また，被控訴人は，同社の取締役または監査役が株式会社Ａの役員に就任するなど，ベネッセグループとして株式会社Ａと一体で事業を行っていた。さらに，被控訴人は，株式会社Ａに本件システムを開発させるにあたり，被控訴人の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月まで株式会社ＡのＩＴソリューション部の部長として兼務させていた。

このような具体的な事情からすれば，被控訴人は，本件システム開発に関する事業について，株式会社Ａ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。

さらに，被控訴人と株式会社Ａとの間の平成２１年１０月１日付業務委託基本契約（甲４２，以下「本件業務委託契約」という。）の内容は，①本件システムの具体的内容の決定権限が委託者（被控訴人）にあること，②本件システムの最終的な動作確認の権限が委託者（被控訴人）にあること，③受託者（株式会社Ａ）が随時，委託者（被控訴人）の担当者に対して運用に関する報告を行うこと，④障害や不具合が発生した場合には，受託者（株式会社Ａ）と委託者（被控訴人）の担当者との間で原因調査や対応策について協議を行うこととされており，本件システムの具体的な内容を発注者である被控訴人が決定することとなっていた。また，株式会社Ａは，被控訴人の発注書等に従って委託業務を処理する義務を負っており（第３条第１項），本件システムの開発やプログラム作成業務が完成した場合，株式会社Ａは，その旨を被控訴人に通知し，被控訴人の検査を受けなければならないものとされ（第８条第１項），被控訴人は，同検査の結果合格と認定したもののみを引き受けるもとされていた（第８条第２項）。そして，同検査が不合格となった場合には，株式会社Ａは，その内容を修正の上被控訴人に再提出し，被控訴人の再検査を受けなければならないものとされ（第９条第１項），また，同検査が不合格のために発注書等の目的が達成できないときには，被控訴人は株式会社Ａとの業務委託契約を解除することができるものとされていた（第９条第３項）。

これらによれば，本件システムの具体的内容の決定権限及び本件システムの最終的な動作確認の権限が委託者（被控訴人）にあったことが認められ，被控訴人と株式会社Ａとの間の実質的な指揮監督関係の存在が認められる。

【被控訴人の主張】

㈠　被控訴人の事業の執行ではないこと

被控訴人は株式会社Ａに本件システム開発の業務を委託し（本件業務委託契約），株式会社Ａは同契約に基づいて業務を行っていたものであるから，それが被控訴人の業務を執行していたことにはならない。

㈡　使用関係（実質的指揮監督関係）がないこと

被控訴人と株式会社Ａとの間の本件業務委託契約には，控訴人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，被控訴人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。

また，被控訴人は，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が，被控訴人が委託元として委託業務の進捗を確認したものに過ぎない。また，被控訴人は，個人情報の保護要件が変更になった場合には，説明会を実施して株式会社Ａの幹部社員に説明を行うほか，ミスやトラブルが発生した場合には，その都度株式会社Ａのセキュリティの設定状況の確認を行っていたことについても，被控訴人が委託元として，個人情報保護のための情報提供や監督を行ったに過ぎず，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。株式会社Ａと被控訴人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のであって，両者は一体となっていたわけではない。

民法７１５条１項本文の「ある事業のために他人を使用する」とは，自らの事業のため他人を補助者として使用していたと同視しうる場合や使用者と被用者との関係と同視し得る関係がある場合を指すものであるところ，上記のとおり，本件業務委託契約における被控訴人と株式会社Ａ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。標準的なシステム開発契約においては，受託者は，独立した立場で，契約に従って業務を遂行しているのであって，何ら委託者の補助者であるとか被用者であるなどとみられる余地はない。

以上のとおり，被控訴人と株式会社Ａ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，被控訴人に使用者責任が成立することはない。

㈢　選任及び監督についての相当の注意について

なお，仮に，被控訴人と株式会社Ａとの間に使用関係が認められるとしても，被控訴人が株式会社Ａの選任及び監督について「相当の注意」（民法７１５条１項但書）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，被控訴人に使用者責任は成立しない。

⑷　争点⑷（全請求）

控訴人に生じた損害の有無及び数額

【控訴人の主張】

ア　被控訴人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。

イ　そればかりか，被控訴人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。

ウ　更に，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，思想等の分析がなされている。かかるビッグデータは匿名化がな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，個人情報を突合することにより，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。

エ　被控訴人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，控訴人は，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。

オ　更に，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。なお，例えばアメリカ合衆国の「児童オンラインプライバシー保護法（ＣＯＰＰＡ）では，１３歳未満の児童を対象としたウェブサイト事業者やオンラインサービス事業者で，自らが収集する情報の主体が児童であることにつき現実の認識を有している者は，その児童の個人情報を収集，利用，開示する際に，その児童の親に対して通知をしなければならず，親の検証可能な同意を義務付けている。このように，児童の個人情報

はより重要なものとして保護すべきであるとされている。

カ　また，被控訴人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。

キ　以上のような事情を踏まえれば，控訴人に対する慰謝料は，１０万円を下ることはない。

【被控訴人の主張】

ア　本件漏えいの対象となった控訴人の本件個人情報は，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（実際に控訴人は，自己の住所・氏名をインターネットに公開していた。），基本情報とされるものであり，不法行為法上の被侵害利益として法的保護の対象となる伝統的なプライバシーの範疇に入るものではない。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る。

そして，たとえ本件漏えいが個人に関する情報をみだりに第三者に開示されないという利益を侵害するもので，不法行為法の被侵害利益の侵害にあたるとしても，株式会社Ａ及び被控訴人の責任は，故意によるものではなく，過失によるに過ぎないものである。

イ　控訴人には，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，また具体的損害，実質的損害が将来発生する蓋然性もない。控訴人の住所や電話番号は，もともと過去に発行された電話帳（紙媒体）に掲載されていたため，本件漏えい当時において，控訴人の住所や氏名は，インターネットにおいて公開されており，現時点でも公開中である（乙８９）。また控訴人の住所氏名は不動産登記情報としても公開されている（乙９０）。本件漏えいにより，控訴人の個人情報（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，広く全世界に公開されているわけではなく，ま

た，本件漏えい当時，控訴人の名前や住所はすでに名簿に登載されて名簿業界にあったことは確実であるから，本件漏えいによって，控訴人の置かれている状況が実質的に変わったものでは全くない。控訴人が，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。

もっとも，プライバシーに係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。

本件で，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，か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。要するに住所，氏名，電話番号といった情報の名簿業者への流出は，それにより営業や宣伝にかかる郵便物が増加し，架電がなされることはあり得るが，しかしそれは紙ゴミが増加し，また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え，それゆえ，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９７３頁）は，プライバシーに係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，同事件と異なって精神的損害（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，プライバシーに係る情報が無断開示され，また，当該プライバシーに係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，本件事案とは全く異なるし，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，秘匿性が高いものでは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撫されるとみて，慰謝料の発生を認めるべきではない。

特に本件においては，控訴人の住所・氏名等は，控訴人の意思に関わりなく流通し，名簿業界内はもちろんのこと，全世界に向けて公開されている現状にあるなか，故意でもない本件事故を理由にして，控訴人に「損害」を認め，被控訴人の行為を違法と評価することは，控訴人の被害填補や救済の効果があるものではなく，控訴人が，その意のままに特定の行為のみ取り上げて罰を与え“制裁”を課すことを許すようなものであり，不法行為法の目的に適うものではなく，その弊害は著しいと言わざるを得ない。

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。

⑴　被控訴人および株式会社Ａ（甲４２，７０）

ア　被控訴人は，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。株式会社Ａは，被控訴人のいわゆるグループ会社（本件漏えい当時は被控訴人の１００％子会社）であり，被控訴人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⑴）

イ　被控訴人は，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（甲１８の２，７０，７３）。

控訴人は，未成年者であるＣが被控訴人の講座等を利用するに際し，被控訴人に対して本件個人情報を提供したもので，被控訴人が，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（弁論の全趣旨）。

ウ　被控訴人は，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使用するシステム（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株式会社Ａに委託した（本件業務委託契約）。（前提事実⑴オ）

被控訴人は，本件業務委託契約において，株式会社Ａ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控訴人が管理する個人情報について株式会社Ａの委託業者の従業員がアクセスすることを認めていた（弁論の全趣旨）。

エ　株式会社Ａは，本件業務委託契約に基づいて委託された業務を，被控訴人の承諾を得て，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，株式会社Ａ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，株式会社Ａ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７０）。

もっとも，株式会社Ａ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，株式会社Ａ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６・７頁）。

なお，Ｂは，株式会社Ａの再委託先業者から業務委託を受けた再々業務委託先の従業員として当該業務に従事する者であったが，本件システム開発業務を行うに際し，許可なく，被控訴人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持ち出したり，同情報を複写・複製したりしてはならないことを約していた（甲１７）。

⑵　本件個人情報の漏えい

業務委託先の従業員であったＢは，平成２４年４月頃から，株式会社Ａ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。そ

こで，Ｂ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，株式会社Ａから貸与された業務用ＰＣを用いて，本件システム開発等の業務に従事していた。（前提事実⑴カ）

Ｂは，平成２６年６月１７日及び同月２７日，株式会社Ａ多摩事業所の執務室内において，業務用ＰＣから，テラターム（バッチサーバを経由して本件データベースにアクセスする場合に必要なフリーソフトであり，インターネット接続により無償でダウンロードされる［甲１９］。）を用いて，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の上，業務用ＰＣに保存し，同ＰＣからＵＳＢケーブルを用いてＢ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）

当時，株式会社Ａ多摩事業所の執務室内においては，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しばしば行われていた。

Ｂ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。Ｂは，上記日時に係る本件漏えいのほかにも不正に取得した顧客等に関する個人情報があり，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６）

⑶　本件スマートフォン

本件スマートフォンは，通信方式がＭＴＰ（メディアトランスファープロトコル〔Ｍｅｄｉａ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ〕の略。パソコ

ンとスマートフォン等を接続する際に用いられる規格〔甲９〕）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。本件スマートフォンがＰＣ（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るものであった（甲９，９９，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。）。

⑷　本件漏えい当時に株式会社Ａが採用していた安全管理措置（甲７０，７１，乙１）

ア　インターネットとの接点

株式会社Ａは，データセンターに設置されている本件サーバ（株式会社Ａが管理する被控訴人のサーバ）と株式会社Ａ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て，インターネット環境でのセキュリティ侵害の脅威を可及的に排除する方針を採っていた。

もっとも，インターネットと接する場面の生じることは避けられないから，株式会社Ａは，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　不正アクセスについて，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。

㈣　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。

㈤　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。

㈥　社外への電子メールを全て保存していた。

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《入館許可証の発行又は臨時入館許可証の貸与を受けた者のみ入室できる。》，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，入退室記録の保存，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。

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。

エ　サーバ（甲６，７０）

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株式会社Ａ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。しかし，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，Ｂ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。

オ　業務用ＰＣに対するセキュリティ対策（甲７４ないし７６）

㈠　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（業務に必要なファイル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。

㈡　業務用ＰＣには，前記のほか，セキュリティソフト「秘文」（本件セキュリティソフト）が導入されており，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，ディスクの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（甲７４）。そして，株式会社Ａでは，自由にそれら「個々のデバイスについて使用制御措置」をオンにすることができたが，リムーバブルメディア，ＣＤ，ＤＶＤ，外付けＨＤＤについて制限措置を採っていたものの，ＷＰＤデバイスについて，その使用を制御する措置は採られていなかった（甲７５，７６）。

また，同ソフトの「書出し制御機能」については，リムーバブルメディア，ＣＤ，ＤＶＤ，外付けＨＤＤについては可能であったが，それ以外のＷＰＤデバイスなどについてはできなかった（甲７５）。したがって，ＭＴＰ対応の本件スマートフォン（ＷＰＤデバイス）への書出しを制御することはできず，制御されていなかった。なお，従前のスマートフォン（データの通信方式にＭＳＣが採られている。）はリムーバブルメディアとして認識されたから，書出し制御の対象とすることができたし，実際にも書出し制御されていた（甲７５）。

ところで，本件セキュリティソフトにつき，株式会社Ａは，平成２３年８月にバージョンアップをしてその設定を完了していたが，それ以降，平成２６年７月までの間，上記セキュリティソフトのバージョンアップを行っていなかった。もっとも，本件漏えい時点での最新のバージョンに設定されていたとしても，本件セキュリティソフトには，通信方式がＭＴＰのデバイス（ＷＰＤデバイス）についての書出し制御機能はなかった（甲７６）。

株式会社Ａは，本件漏えい後，本件セキュリティソフトのバージョンアップをするとともに，その設定を見直し，平成２６年７月２２日以降は，リムーバブルメディア，ＣＤ，ＤＶＤ，外付けＨＤＤについては従前どおり書出し制御の措置を採り，他のデバイスについては，プリンタ，ネットワークドライブ，無線ＬＡＮ，パラレル／シリアルポート以外の

ものについて，使用可否制御をすることにより使用することができない設定とした。これにより，本件スマートフォンのようなＭＴＰ対応機器（ＷＰＤデバイス）を接続しても，これらを使用することができなくなり，それらの機器を外部記録媒体として，データを書き出すこともできなくなった。（甲７６）

カ　データ

本件サーバ上の一定の重要なデータについては暗号化し，また，ＳＱＬログの記録（データベースにアクセスした記録）を全て取得して保管していた。

キ　顧客情報の機密指定，研修等

株式会社Ａでは，同社が取り扱う被控訴人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（被控訴人においても，被控訴人の顧客情報を機密情報と位置付けていた。）。また，株式会社Ａ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，さらに，毎年，業務従事者（株式会社Ａ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。

２　本件個人情報の被侵害利益性

⑴　本件漏えいによって流出した本件個人情報の内容は，Ｃの氏名，性別，生年月日，郵便番号，住所，電話番号，保護者名（控訴人の氏名）及び控訴人とＣとの続柄であるところ，まず，Ｃの郵便番号，住所，電話番号は，Ｃが本件漏えい当時１０歳に満たない未成年者であったことからすると，控訴人自身の郵便番号，住所，電話番号でもあると推認できること，また，Ｃの氏

名，性別，生年月日は，控訴人の個人情報そのものではないとしても，控訴人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，控訴人の氏名はもちろんのこと，その他の情報も控訴人の個人情報であると認められる。

そして，本件個人情報は，これを全体としてみれば，控訴人のプライバシーに係る情報として法的保護の対象となるというべきである（本件上告審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）。

⑵ そして，被控訴人から本件業務委託契約に基づいて本件業務を委託された株式会社Ａの業務委託先の従業員であったＢは，被控訴人（株式会社Ａ）が控訴人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控訴人の本件個人情報を，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ものであるから，控訴人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ものと認められる。

３ 争点⑴（本件漏えいについての株式会社Ａ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

ア㋐ 証拠（甲７，８，１６，１９，２１）によれば，①安全対策基準（旧通商産業省の平成９年のもの）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とともに，その内容を確認し，記録をとること」と記載されていたこと，②平成１８年のＪＩＳＱ１５００１及び平成２２年のマネジメントシステム実施ガイドラインにおいては，「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掲げられていたこと，③平成２１年の経済産業分野ガイドラインには，

「個人データを入力できる端末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こと，④平成２５年の内部不正防止ガイドラインにおいては，「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こと，⑤平成２５年のデータセンターセキュリティガイドブックにおいては，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ことが認められ，これらによれば，本件漏えい以前から，外部記録媒体をパソコン等に接続する方法による情報漏えいのリスクが指摘されていたことが認められる。

また，前記認定のとおり，株式会社Ａは，複数のアカウントの設定や監視など厳重なセキュリティ対策を講じていた上，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出し制御が実施されている旨を周知させており，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し，本件漏えい時点において，ＭＴＰ対応のスマートフォン以外の外部記録媒体に対して，書出し制限措置ないしデバイス使用制御措置を採っていたことが認められる。

これからすると，株式会社Ａ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。

㈠ また，証拠（甲１０，５０，５１，乙３６）によれば，平成２５年１月時点において，ＯＳが「Ａｎｄｒｏｉｄ」であるスマートフォンの契約数２５７０万件のうち半数を超える１２３５万件以上が「Ａｎｄｒｏｉｄ４．０」以上のバージョンの「Ａｎｄｒｏｉｄ」端末（ＭＴＰ対応のスマートフォン）であったこと，当時の一般的なセキュリティソフトがＷＰＤ使用制限機能（通信方式がＭＴＰである機器はＰＣのウィンドウズ上ではＷＰＤデバイスとして扱われるので，ＭＴＰ対応機器を使用制限するには，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。）に対応した時期は，別紙（添付省略）のとおりであり，また，それら各製品の国内市場におけるシェアが，本件漏えいのあった平成２６年６月時点で合計すると４３．５％以上であったことが認められる（なお，株式会社Ａが業務用ＰＣに導入していた本件セキュリティソフトは，ＭＴＰ制御機能として，未登録デバイスの使用制御ができるものであったが，読み取り専用の設定とすることはできないものであった《乙３６》。）。

㈡ そして，株式会社Ａは，被控訴人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，事業用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，株式会社Ａ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，事業用ＰＣにＵＳＢを接続して充電を行うことを容認していたのであるから，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，あるいは認識しえたと認められる。

㈡　そうであるとすれば，株式会社Ａ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であるスマートフォンについては個人情報を不正に取得されることがないように本件セキュリティソフトによって書出し制御の措置を採っていたというのであるから，スマートフォンを業務用ＰＣ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があること自体は認識していたもので，当時，多数のＭＴＰ対応スマートフォンが国内市場に出回っていたのであるから，執務室内で作業する従業員が，ＭＴＰ非対応スマートフォン（通信方式がＭＳＣであるスマートフォン）だけでなく，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される可能性があることを認識し得たものと認められる。

イ　この点，被控訴人は，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もので，株式会社Ａには本件漏えいについての予見可能性は認められないと主張するので，以下検討する。

㈠　①について

「携帯電話端末におけるＭＴＰ普及率についての調査報告」（乙３５）

には，スマートフォンと従来の携帯電話を併せた台数に対するスマートフォンの割合は，平成２４年３月末で２２％，平成２５年３月末で３６％，平成２６年３月末で４８％であり，ＭＴＰ対応のスマートフォン（「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２４年６月時点で０．６９％，平成２５年６月時点で１９．８８％，平成２６年６月時点で２１．４１％であったこと，また，平成２６年のスマートフォンの出荷台数が２７７０万台であったことが記載されている。これによれば，平成２６年６月頃のＭＴＰ対応のスマートフォンの台数は，５９３万台余りあったということになる。そして，スマートフォンの契約件数が増加傾向にあり，同年１２月末の時点で６５４４万件になることが見込まれていたこと（乙３５の資料１）や，前記アにおいて認定したとおり，ＭＴＰ（ＷＰＤ）対応のセキュリティソフトの国内販売シェアが４割以上であったことからすると，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控訴人の主張によっても，株式会社Ａ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ものとはいえない。

(イ) ②について

端末管理・セキュリティ製品におけるＭＳＣ・ＭＴＰ制御機能についての調査報告（乙３６）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ところ，上記定義に該当するような設定ができれば便宜ではあるが，かならずしもそれがないことをもって実用的でないと評価し得るものではなく，そもそも一般的なＷＰＤデバイスの使用制御機能は前記アにおいて認定したとおり，国内シェアの合計が４割を超える日本電気株式会社等の７つの商品が本件漏えい以前の時期に備えていたし，また，通信方式がＭＴＰである機器はＰＣのウィンドウズ上ではＷＰＤデバイスとして扱われるので，ＭＴＰ対応機器を使用制限するには，ＷＰＤデバイスを使用制限することで可能となるのであるから，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，被控訴人の主張は採用できない。

(ｳ) ③について

被控訴人は，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なされておらず，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（役職名省略）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（役職名省略）を務めるＥの意見書（乙３３「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，ユーザーである株式会社Ａ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３７，３８）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，被控訴人及び株式会社Ａ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控訴人も認めるとおりであり，本件漏えいの時点における状況に照らして，株式会社Ａが，ＭＴＰ非対応スマートフォンだけでなく，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ことは前記アで認定したとおりであって，これらの点は，前記判断を左右するものではない。したがって，これらの被控訴人の主張は採用できない。

なお，前記認定のとおり，本件システム開発業務が行われていた株式会社Ａ多摩事業所の執務室内には，株式会社Ａの業務委託先の従業員による私物の携帯電話やスマートフォンの持込み及び使用が自由に行われており，これらを，充電のために業務用ＰＣのＵＳＢポートに接続することもしばしば行われていたものであるところ（なお，Ｂが自己所有の本件スマートフォンが外部記録媒体となり得ることに気付いたのも，同スマートフォンを充電のために業務用ＰＣにＵＳＢケーブルを接続したことによるものであった。），株式会社Ａは，自己の事業所内の執務室で行われていた以上のような業務委託先の従業員による私物スマートフォンの使用等の状況を当然に認識していたものと認められる。

そして，前記認定のとおり，株式会社Ａは，自己の従業員以外の業務委託先の従業員に株式会社Ａ多摩事業所の執務室内で委託業務を行わせ，これらの従業員が執務室内の業務用ＰＣを使用して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のであるから，以上によれば，株式会社Ａは，個人情報にアクセスすることができる業務用ＰＣに，業務委託先の従業員が，個人所有のスマートフォンをＵＳＢポートに接続することについては，これを容認していたものであるといわざるを得ない。

ところで，株式会社Ａが，本件漏えい当時，少なくとも，通信方式がＭＳＣである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た上で不正取得を防止するための対応をとっていたことは前記認定のとおりであり，そのような中で，株式会社Ａにおいて，上記のように個人所有のスマートフォンを業務用ＰＣに接続することを容認する以上は，本件漏えい当時，業務委託先の従業員が持ち込む可能性のあるすべての私物スマートフォンについて，それが業務用ＰＣのＵＳＢポートに接続されることで個人情報を不正に取得されるリスクがあるか否かを日常的に調査確認し，そのリスクがあれば，これを防止する措置を講ずべき必要性を認識していたものと認められる。

そして，本件漏えい当時においても，株式会社Ａが，以上の点について必要な調査確認を行っていれば（本件セキュリティソフトの製作業者に確認するなど），ＭＴＰ対応のスマートフォンが流通していたことを容易に把握することができたと認められ，このようなスマートフォンが業務用ＰＣのＵＳＢポートに接続されることによって個人情報を不正に取得されるリスクがあることや，本件セキュリティソフトによって，そのリスクを回避できるか否かを容易に認識しえたと認められるから，そ

の意味においても，株式会社Ａには，本件漏えいの危険性について予見可能性があったというべきである。

ウ　以上によれば，株式会社Ａ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対応の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。

(2)　次に，被控訴人は，株式会社Ａに，上記(1)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，控訴人の主張する各措置を講ずべき義務を負うものではないと主張するので，この点について検討する。

本件漏えいは，本件システム開発等の業務委託先の従業員であったＢが，被控訴人ないし株式会社Ａが管理していた本件個人情報を含む大量の個人情報を不法に取得して第三者に売却することを意図して行った故意の不法行為であるところ，被控訴人ないしは株式会社Ａが，本件システム開発等の目的から，Ｂら業務委託先の従業員に，本件個人情報を含む大量の個人情報へのアクセスを認めていたことが要因となって本件漏えいを生じたものと認められる（なお，本件において，控訴人が，本件個人情報を被控訴人に提供するにおいて，同情報を被控訴人以外の第三者に取り扱わせることを包括的に承認していたとの事情は認められない。）。

そして，本件漏えいは，外部と繋がるインターネット環境を利用した不正アクセス等によって行われたという態様ではなく，被控訴人ないし株式会社Ａから株式会社Ａ多摩事業所の執務室内で個人情報に接することを許された株式会社Ａの業務委託先の従業員であるＢによって行われた，犯罪者が特定されることを意に介さずになされた情報侵奪とその漏えい事案であったもので，このような者による本件漏えいを防止するためには，そもそも犯罪抑止効果を狙ってのセキュリティシステムである監視カメラやアラートシステム

の設定といった措置は効果がないというべきであって，このような者に対応した予防措置としては，株式会社Ａにおいて，スマートフォンの持込み禁止の措置，書出し制御措置（ＷＰＤデバイス使用制御措置），物理的にＵＳＢポートを塞ぐなどの接続禁止措置を採るべき義務を負っていたといえるかどうかが問題となる。なお，最後の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が接続することができなくなり，制約として過度なものであって，現実的措置とはいえない。そこで，株式会社Ａが，本件漏えいという結果を回避するために，それ以外の２つの措置を採るべき義務を負っていたと認められるかについて検討する。

ア　スマートフォンの持込み禁止

㈠　前記⑴で認定したとおり，株式会社Ａは，本件漏えい当時，委託先の従業員が私物のＭＴＳ対応スマートフォンを株式会社Ａ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ところ，株式会社Ａ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，株式会社Ａ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，株式会社Ａが，Ｂ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さえいれば，本件漏えいを回避することができたといえる。

そうすると，株式会社Ａは，本件漏えい当時，被控訴人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ていたところ，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を容認していたというのであるから，

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っていたというべきであり，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。

㈠ 付言するに，確かに，Ｂの担当していた業務が，機密性の高い個人情報等の情報を扱う業務というよりも，基本的には通常の事務作業であるというようなものであったならば，私物のスマートフォンの持込みを一切禁止するというのは，当該執務環境において従事する者にとって，非常に大きな制約となる場合があると思われる。しかし，Ｂ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った。そのような業務の内容からして，Ｂ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，Ｂは，その執務していた場所こそ執務室であったが，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，Ｂが作業していた同じ執務室内で他の従業員がどのような業務を担っていたのかは明らかでなく，仮に他の従業員が通常の事務作業を行っていたとしても，少なくともＢについては，機密性の高い個人情報である本件データベースを扱って本件システムを開発する業務を行っていたのであるから，同

人がその私物のスマートフォン（外部記録媒体になり得る。）を持ち込むことを許してはならず，株式会社Ａにおいて，本件漏えい当時，Ｂ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（なお，仮に，執務室内でのスマートフォンの使用が必要な事情があれば，私物のスマートフォンを禁止したうえで，株式会社Ａが貸与するスマートフォンを利用させる方法も考えられるところである。）。

㈣　そして，以上のとおり，株式会社Ａ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スマートデバイス等のモバイル機器及び携帯可能なＵＳＢメモリ等の外部記録媒体の業務利用及び持込みを制限しなければならない旨の指摘があ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１６）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，被控訴人は，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１４）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，被控訴人は，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とする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７）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ことに照らすと，データセンターセキュリティガイドブックの記載は，場所により区分しているものと解されるが，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，Ｂ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。

イ　書出し制御措置及びＷＰＤデバイス使用制御措置について

ところで，控訴人の注意義務違反の主張は選択的であるから，本件においては，その余の義務違反については検討するまでもないところであるが，株式会社Ａ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⑴で判断したとおり，株式会社Ａ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ないし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，被控訴人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，前記⑴イ記載のとおり，ＭＴＰ対応スマートフォン（ＷＰＤデバイス）への書出し制御機能を有するセキュリティソフトは，本件漏えい当時，日本国内で入手可能な状況にあったし，ＷＰＤ使用制御機能は被控訴人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。

㈠ そうであるのに，株式会社Ａは，リムーバブルディスク，ＣＤ／ＤＶＤ，外付けハードディスクについてのみ使用制御の措置を採っていただけで，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，本件セキュリティソフトにより，特定のＵＳＢメモリ以外は全てが使用できなくなっていると思っていたために（甲７５），上記対策をとることを怠っていたことが認められる。

㈡ この点，被控訴人は，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株式会社Ａや被控訴人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，被控訴人（株式会社Ａ）は，本件個人情報を含む大量の個人情報を扱っていたものであるところ，上記⑴で認定のとおり，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ないし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という不便を生じることになる。しかし，株式会社Ａにおいて，本件システム開発等の業務を遂行するにつき，Ｂが使用する業務用ＰＣに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（株式会社Ａや被控訴人のスタンスとして，広く制御するという考え方をとっていなかったというにすぎない。）。現実にも，本件漏えい後の平成２６年７月１４日以降，株式会社Ａは，対応策として，ＷＰＤデバイス，イメージングデバイスその他の制御対象デバイスの使用を制御する措置を採ったというのであるから，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，株式会社Ａ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，株式会社Ａ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。

㈡ 以上，株式会社Ａ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　以上のとおり，本件漏えい当時，株式会社Ａには，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ないしはこれに対する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て，本件漏えいを生じさせた過失があったと認められる。

そうである以上，株式会社Ａは，上記の各注意義務に違反して本件個人情報をＢに利用させたことにより，Ｂの故意による本件漏えいを生じさせたものであり，控訴人に対し，Ｂと共同して不法行為責任を負うべき立場にあると認められる。

４　争点⑵（本件漏えいについての被控訴人の過失）について

⑴　本件漏えいの予見可能性

本件個人情報を含む大量の個人情報を管理して営業に利用してきた被控訴人においても，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ことは，前記３⑴において，株式会社Ａについて記載したところと同様である。

そこで，以下，被控訴人が，控訴人の主張する各措置を採らなかったことについて，注意義務違反が認められるかを検討するに，控訴人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，かかる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，株式会社Ａに対するのと同様のスマートフォン持込み禁止等にかかる種々の注意義務については，本件漏えい当時，株式会社Ａが被控訴人の１００％子会社であったというだけでは，株式会社Ａの過失を被控訴人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控訴人の過失をいう控訴人の主張は理由がなく，結局，委託先選任及び監督にかかる注意義務違反が

あるか否かを検討することになる。

⑵　委託先選任及び監督にかかる注意義務違反について

ア　被控訴人は，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，業務委託先である株式会社Ａ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ものである（なお，被控訴人が，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。）。

イ　ところで，個人情報保護法２２条は，「個人情報取扱事業者は，個人データの取扱いの全部又は一部を委託する場合は，その取扱いを委託された個人データの安全管理が図られるよう，委託を受けた者に対する必要かつ適切な監督を行わなければならない。」と規定し，経済産業分野ガイドライン（甲８）には，「必要かつ適切な監督」に関し，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２１）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。」等と規定し，マネジメントシステム実施ガイドラインは，「審査

の着眼点」として，「委託先を選定する基準として，該当する業務については少なくとも自社と同等以上の個人情報保護の水準にあることを客観的に確認できること，選定基準は具体的で運用可能なものであること」等を例示している。

そして，以上によれば，大量の個人情報の運用管理を株式会社Ａに委託していた被控訴人には，本件漏えい当時，個人情報の管理について，委託先に対する適切な指導監督をすべき注意義務があったところ，前記⑴記載のとおり，被控訴人は，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にもかかわらず，株式会社Ａ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，株式会社Ａの業務委託先の従業員が，被控訴人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もので，これらについて適切に指導監督を行っていれば，ＭＴＰ対応スマートフォンに対する書出し制御機能に対応したセキュリティソフトへの変更を指示するか，あるいは，本件セキュリティソフトのままであっても，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たものであり，それが困難であったとしても，株式会社Ａ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，被控訴人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，被控訴人には，本件漏えい当時，株式会社Ａにおける被控訴人の有する個人情報の管理につき，セキュリティソフトの変更や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，被控訴人は，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，被控訴人が，株式会社Ａ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２４の２）。

ウ　この点，被控訴人は，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株式会社Ａに対する委託先監督を実施していた旨主張する。しかし，被控訴人は，大量の個人情報の運用管理を株式会社Ａに委託して，被控訴人と直接の契約関係のない株式会社Ａ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もので，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，株式会社Ａ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) 以上のとおり，被控訴人は，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るところ，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株式会社Ａに対する適切な監督義務に違反した結果，Ｂによる本件漏えいを生じさせたものと認められるから，控訴人に対

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。

そして，被控訴人と株式会社Ａの不法行為（及びＢの本件漏えいによる不法行為）は，被控訴人が保有し，その管理を株式会社Ａ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）。

そうである以上，控訴人が選択的に主張する被控訴人の株式会社Ａに対する使用者責任（争点⑶イ）並びにＢの本件漏えい行為を不法行為としてそれに対する株式会社Ａ及び被控訴人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。

５　争点⑷（控訴人に生じた損害の有無及び数額）について

⑴　前記２で判断したとおり，本件個人情報は，控訴人のプライバシーに係る情報として法的保護の対象となるというべきであるから（本件上告審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），上記認定事実によれば，本件漏えいによって，控訴人はそのプライバシーを侵害されたと認められる。

そして，本件漏えいは，経済的に困窮したＢが，本件個人情報を含む大量の個人情報を名簿業者に売却して金銭を得る目的で行ったものであるところ，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藉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。

⑵　本件で流出した個人情報の内容は，Ｃの氏名，性別，生年月日，郵便番号，住所，電話番号，保護者名（控訴人の氏名）及び控訴人とＣとの続柄である

ところ，まず，Ｃの郵便番号，住所，電話番号は，Ｃが本件漏えい当時１０歳に満たない未成年者であったことからすると，控訴人自身の郵便番号，住所，電話番号でもあると推認できること，また，Ｃの氏名，性別，生年月日は，控訴人の個人情報そのものではないとしても，控訴人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，控訴人の氏名はもちろんのこと，その他の情報も控訴人の個人情報であると認められることは前記２で判断したとおりである。

次に，これらの情報のうち，控訴人の氏名，郵便番号，住所及び電話番号は，いずれも控訴人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（実際に，証拠《乙８９及び９０》によれば，控訴人の住所・氏名及び電話番号はホームページ上に開示されており，その住所及び氏名は不動産登記情報にも記載されている。）。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惧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，子の氏名，性別，生年月日及び控訴人との続柄については，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。

(3) ところで，本件個人情報は，情報流出元が被控訴人という教育関係の会社

であったことや控訴人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，控訴人にとって，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。もっとも，控訴人においても，現時点では，個人情報を利用した詐欺などの具体的な金銭被害は生じていないとし，ダイレクトメールや勧誘の電話が増加することは顕著な事実であると主張するだけで（控訴人第４準備書面），現実にそれらが増えたという主張はなく，したがって，ダイレクトメールが増大するなどして，控訴人に何らかの実害が生じたことはうかがわれない（なお，もともと，本件個人情報は，Ｃの個人情報として被控訴人に提供されたものであり，本件漏えいによってＣ個人に生ずる精神的苦痛による損害も想定されるところ，Ｃと控訴人が同居していることを踏まえても，これを控訴人の損害として考慮することは相当ではない。）。

しかし，その流出範囲については，本件漏えいにより，二次的拡散も発生しており５００社を超える名簿業者等に情報が漏えいしたとの発表があり（甲４６），被控訴人においてもそれを確認する術がない状況にあって，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。被控訴人に個人情報を開示した顧客の一人である控訴人にとって，控訴人の承諾もないままにＢ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控訴人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侵害行為であるというべきである。

この点，被控訴人は，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，具体的に名簿利用による勧誘や電話

により日常生活に支障を及ぼすなどの損害が発生したときには，それが本件漏えいと相当因果関係のある損害であることを立証して損害賠償請求できることはもちろん，それに至らない場合であっても，本件個人情報を利用する他人の範囲を控訴人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，控訴人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。

(4) 他方，被控訴人の持株会社であるベネッセホールディングスは，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，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ていたことが認められる。

(5) そうすると，控訴人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，本件個人情報が控訴人の子であるＣの個人情報として被控訴人に対して提供されたもので，控訴人の住所・氏名・電話番号はホームページなどで開示されていたことなど，本件に顕れた一切の事情を考慮すれば，控訴人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。

第４　結論

以上によれば，控訴人の請求は，１０００円の支払を求める限度で理由があるから，その範囲で認容し，その余は理由がないから棄却すべきところ，これと異なり，控訴人の請求を全部棄却した原判決は失当であって，本件控訴の一部は理由があるから，原判決を上記のとおりに変更することとして，主文のとおり判決する。

大阪高等裁判所第１３民事部

裁判長裁判官　　木　　納　　敏　　和

裁判官　　山　　本　　善　　彦

裁判官　　木　　上　　寛　　子