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，選定者Ａのために２０００円，選定者Ｂのために２０００円，選定者Ｃのために２０００円及びこれらに対する平成２６年６月２８日から各支払済みまで年５分の割合による金員をそれぞれ支払え。

(2) 控訴人のその余の請求をいずれも棄却する。

2　訴訟費用は，第１，２審を通じて，これを２５分し，その１を被控訴人の，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，選定者Ａ（以下「控訴人」という。）のために５万円，選定者Ｂ（以下「選定者Ｂ」という。）のために５万円，選定者Ｃ（以下「選定者Ｃ」という。）のために１０万円及びこれらに対する平成２６年６月２８日から各支払済みまで年５分の割合による金員をそれぞれ支払え。

第２　事案の概要

1　本件は，被控訴人に個人情報を提供した選定者らが，控訴人を選定当事者として（以下，控訴人，選定者Ｂ及び選定者Ｃを併せて「控訴人ら」という。），被控訴人が株式会社シンフォーム（以下「シンフォーム」といい，被控訴人とシンフォームを併せて「被控訴人ら」という。）にその管理を委託し，シンフォームが更に外部業者に再委託し，再委託先の従業員が当該個人情報を外部に漏えい（以下「本件漏えい」という。）させたことにつき，①被控訴人らにおいて控訴人らの個人情報の管理に注意義務違反があった，②シンフォームは上記従業員の使用者であり，上記従業員の行為はシンフォームの事業の執行についてされたものであるところ，被控訴人はシンフォームの使用者であり，シン

フォームの注意義務違反は被控訴人の事業の執行についてされたものであり，本件漏えいにより控訴人らは精神的苦痛を被ったと主張して，被控訴人に対し，不法行為に基づき，慰謝料として控訴人及び選定者Ｂについてそれぞれ５万円，選定者Ｃについて１０万円及びこれらに対する情報流出のあった日の後の日である平成２６年６月２８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。

２　原審は，被控訴人に委託元の個人情報取扱業者として個人データの漏えいについて過失があったことを認めるに足りる具体的事実の主張・立証がないとして，控訴人の請求を棄却した。そこで，控訴人がこれを不服として控訴した。

第３　前提事実（争いのない事実，掲記の証拠（以下，枝番のある書証は枝番を含めて表記する。）及び弁論の全趣旨により容易に認められる事実）

１　当事者等

(1) 控訴人は，選定者Ｂの夫であり，選定者Ｃの父である。選定者Ｃは，本件訴訟提起当時２歳７カ月であった（弁論の全趣旨）。

(2) 被控訴人は，通信教育，模擬試験や雑誌の発行・通販事業を行う株式会社である。

シンフォームは，被控訴人のいわゆるグループ会社であり，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。

(3) 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多くなったことから，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（以下「本件システム」といい，同システムのデータベースについては「本件データベース」という。）を構築することとして，本件システム構築等の業務（以下「本件業務」という。）をシンフォームに委託した。

シンフォームは，その運用及び保守管理を，更に複数の外部業者に分散して再委託していることがあった。

シンフォームは，毎年，シンフォームの業務に従事する者（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き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，その研修内容を踏まえたテストを実施していた。

(4) 控訴人及び選定者Ｂは，被控訴人に対し，自ら及び選定者Ｃの氏名及び住所等の個人情報（以下「本件個人情報」という。ただし，その具体的内容については，後記のとおり，当事者間に一部争いがある。）を提供し，本件個人情報は，本件データベースに保存されていた。

２　本件システム及び本件データベース

(1) 本件システムにおいては，前記１(3)の顧客管理のシステムや販売管理のシステム等の本件システムと連携するシステム（以下「連携システム」という。）に集積された顧客情報が，まず本件データベース内の「インポート層」と呼ばれるデータ領域に保存され，次いで「インポート層」内のデータの形式を揃えるなどの加工がされたデータが「ＤＷＨ層」と呼ばれるデータ領域に保存され，さらに当該データの個人を特定する情報を捨象して分析ソフトで分析しやすい形式にするなどの加工をしたデータ（個人情報を有しないデータ）が「マート層」と呼ばれるデータ領域に保存される仕組みとなっていた。そして，本件システムの運用開始後は，被控訴人の事業部門は，分析ソフトを使用し，個人を特定する情報が捨象された「マート層」に保存されたデータを活用することになっていた。

(2) 本件システムの開発作業においては，「インポート層」，「ＤＷＨ層」及び「マート層」の各層ごとに，顧客情報が保存されていたデータ領域である「本番環境」と運用開始前の各種テストを実施するために使用されるデータ

領域である「開発環境」が存在したところ，「開発環境」と「本番環境」はそれぞれ物理的に切り離されていた。そして，「開発環境」においては，個人情報を含んだデータの保存はされず，ダミーデータやマスキングデータが用いられることになっていた。また，ネットワークが業務単位ごとに分離され，業務上必要なサーバへのみアクセスが可能なようにアクセス制御が行われていた。

(3) 本件システムは，更にその領域ごとにアカウント管理がされていた。すなわち，本件データベースの「インポート層」，「ＤＷＨ層」及び「マート層」の各層における「本番環境」及び「開発環境」のいずれの環境にアクセスする際にも，それぞれ別個に設定されたアカウントが必要であった(以下，各環境での作業も含め，本件システム開発等の業務に要するアカウントを総称して，「本件システムのアカウント」という。)。

本件システムのアカウントには，個々の業務従事者を対象に発番されるアカウント（以下「個人用アカウント」という。）と，本件システムの開発，運用及び保守等に関連する業務を対象に発番され，当該業務に従事する複数の業務従事者が共同で使用するアカウント（以下「業務用アカウント」という。）があり，業務用アカウントには，本件システムに直接アクセスする際に使用されるもののほか，プログラム構築等の効率化のためのバッチサーバ（バッチ処理〔一定量のデータを集め，一括処理する方法〕を行うサーバ）にアクセスする際に使用されるものも存在した。

被控訴人らにおいて，本件システム及び連携システムの各データベースに集積されている顧客情報にアクセスするには，本件システムのアカウント使用の承認が必要であり，個人用アカウント及び業務用アカウントの新規発番は，いずれも，当該システムの担当部門の上長である課長が，発番の必要性等を判断し，その上位の部長の承認を受けた上，同部門から発番を担当するインフラ部門に対して申請を行い，発番を受けるという流れで行われていた。

本件システムのアカウントの提供を受けていたのは，シンフォームにおいては，本件システムに関する開発，運用及び保守等の業務並びに連携システムに関する業務の担当者であり，また被控訴人においては，対応窓口になっていたＩＴ戦略部等の本件システムの担当者等であった。

本件システムの開発等の業務担当者は，本件データベースにアクセスするために，会社から貸与された業務用パソコンから直接本件データベースの顧客情報等のデータにアクセスする場合と，プログラム構築等の効率化のためのバッチサーバを経由してアクセスする場合があったところ，業務用パソコンから，本件データベース内の顧客情報に直接アクセスする場合には訴外オラクルのソフトウェアが，バッチサーバを経由してアクセスする場合はテラターム（インターネット接続が可能であれば，無償でダウンロード及びインストールが可能なフリーソフト〔甲１８〕）というソフトウェアが，それぞれ必要であった。

３　本件漏えい

(1) シンフォームの再委託先の外部業者の社員であった訴外W（以下「W」という。）は，平成２４年４月頃から，シンフォーム東京支社多摩事務所（以下「シンフォーム多摩事務所」という。）において，本件業務に従事するようになった。Wは，本件業務に従事する複数の担当者が本件システムや連携システム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，シンフォームから貸与された業務用パソコンを用いて，本件業務に従事していた。

(2) Wは，平成２５年７月頃ないし平成２６年６月頃，シンフォーム多摩事務所において，業務用パソコンから，テラタームを用いて，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，業務用パソコンに保存し，ＵＳＢケーブルを用いてW所有のスマートフォン（以下「本件スマートフォン」とい

う。）に転送し，その内蔵メモリに保存する等の態様により不正に取得した。本件スマートフォンは，ＭＴＰ（メディアトランスファープロトコル〔Ｍｅｄｉａ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｃｏｌ〕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１１〕）に対応していた。

なお，当時，シンフォームの業務においては，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，充電のために，スマートフォンを業務用パソコンにＵＳＢケーブルで接続することも許容されていた。

(3) Wは，不正に取得した上記個人情報の全部又は一部を，名簿業者３社に対して，それぞれ売却したところ，本件個人情報も，少なくとも，そのうちの１社に売却された（本件漏えい）。

(4) Wが不正に取得した顧客等に関する個人情報は，延べ約２億１９３９万件であり，同一人物と見られる個人情報を名寄せし，重複を解消したとしても，約４８５８万人分であった。

４　本件漏えい当時にシンフォームが採用していた安全管理措置（乙１）

(1) インターネットとの接点

シンフォームは，データセンターに設置されているサーバとシンフォームの執務室内のパソコン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ていなかった。また，シンフォームは，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。

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。

(2) 物理的境界

個人情報が保管されているサーバは，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管理（入館の事前申請・入館制限，私物持ち込み不可，機器持ち出し不可及び監視カメラ設置等）が行われており，また，業務を行う執務室についても入退室管理（申請制による入退室制限，入退室記録の保存及び入退室に係る箇所への監視カメラの設置等）が行われていた。

(3) 内部ネットワーク

前記２(2)のとおり，本番環境と開発環境の分離がされていたほか，ネットワークが業務単位に分離され，業務上必要なサーバへのみ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，拠点からは管理に必要なプロトコルのみ許可し，私物パソコンの社内ネットワーク接続が禁止され，業務用パソコン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。

(4) サーバ

本件データベースのサーバに関しては，アカウント管理が行われ，「踏み台サーバ」としてバッチサーバを経由させた上で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。

また，シンフォームにおける連携システムのデータベースサーバにつき，シンフォームの業務を行う担当者が使用するクライアントパソコンから個人情報が記録保管されているサーバへのアクセスは，自動的にアクセスログ及び通信ログが記録されるように設定されていた。

さらに，クライアントパソコンと連携システムのデータベースサーバの間

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。しかし，クライアントパソコンと本件データベースとの通信については，W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が講じられていなかった。

(5) 業務用パソコンに対するセキュリティ対策

ア　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パソコンとを分け，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，業務用パソコンについて設定されていたセキュリティ対策としては，①ウイルス対策ソフトの搭載，②ＵＲＬ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，③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送信を差し止める。）の設定，④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，⑤パスワードの設定等があった。

イ　業務用パソコンには，前記アのほか，セキュリティソフトが導入されており，その主な機能は以下のとおりであった。

㈠　操作ログの記録

㈡　ＵＳＢ等の外部記録媒体への書き込み制御

㈢　ディスクの暗号化

(6) データ

一定の重要なサーバ上のデータについては暗号化し，また，ＳＱＬログの記録を全て取得して保管していた。

5　本件漏えい後の被控訴人の対応（甲１，１７）

(1) 本件漏えいの発覚

被控訴人は，平成２６年６月下旬，顧客から，被控訴人だけに登録した情

報でダイレクトメールが届いているなどの問合せが急増したことから，自社の顧客の個人情報が社外に漏えいしている可能性を認識し，同月２７日に調査を開始して，同月２８日，原因究明の調査及び顧客対応等のため緊急対策本部を設置するとともに，同月３０日，経済産業省に状況を報告して対応を相談し，警察にも対応を相談するなどした。

被控訴人は，同年７月７日，シンフォームにおいて大量の顧客情報が漏えいした形跡があることを把握し，警察に捜査を依頼した。

(2) 本件漏えいの公表等

被控訴人は，同月８日，その保有する顧客情報を用いて作成された名簿に基づき勧誘活動を行っている企業及び名簿を取り扱っている名簿業者に対して名簿の利用及び販売の中止を求める内容証明郵便を送付し，同月９日，本件漏えいの事実を公表した。

(3) その後の報告，公表及び補償等

ア　被控訴人は，同月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。

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どもたち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１７）。

控訴人らは，いずれも上記の電子マネーギフト５００円分を受領した（なお，被控訴人は，選定者Ｃが，更に電子マネーギフト５００円分（合

計１０００円分）を受領した旨を主張するが，これを認めるに足りる証拠はない。）。

エ　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Ｖ会長兼社長（当時）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。

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交付し，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。

上記事故調査報告書においては，「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」について，①アラートシステム，②クライアントパソコン上のデータのスマートフォンへの書き出し制御設定，③アクセス権限の管理，④データベース内の情報管理が指摘された。

第４　争点及びこれに関する当事者の主張

１　本件漏えいについてシンフォームに過失があったか否か（争点１）

（控訴人の主張）

(1)　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ち込み自体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。

㋐　「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。）においては，「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，…外部記録媒体を接続できないようにする)」ことが望ましいと規定されていた。

㋑　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。）においては，「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」と記載されていた。

㋒　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。）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いたほか，重要情報を扱う物理的区画のセキュリティ強化として，カメラ等で監視及び監視している旨を伝えることが記載されていた。

㋓　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。）においては，ＵＳＢメモリ等の情報記憶媒体や携帯電話の持ち込み・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。

㋔　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（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９月１７日。以下「マネジメントシステム実施ガイドライン」という。）においては，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業務上の必要性に基づく限定対策として掲げられていた。

イ　また，シンフォームは，毎年，正社員及び再委託先の外部業者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き出し制御が実施されている旨周知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リスクを十分把握していた。

ウ　Wが本件漏えいを行った際に使用したスマートフォンは，平成２４年１２月頃に発売が開始され，ＭＴＰに対応したスマートフォンであった。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，代表的な商用デバイス制御ソフトが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，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。

(2) 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った（各主張はいずれも選択的）。

ア　私物スマートフォンの持ち込みに係る注意義務違反

安全対策基準は，個人情報を取り扱う企業にとって最低限の基準であり，これに違反した場合には，注意義務違反があったと解すべきである。また，内部不正防止ガイドラインは，企業やその他の組織において必要な内部不正防止対策を効果的に実施可能とすることを目的として，内部不正の知見を有する有識者で構成された「組織における内部不正防止ガイドライン検討委員会」において作成されたものであるから，同ガイドラインで要求する事項を考慮していない場合には，注意義務違反があったと解すべきである。さらに，データセンターセキュリティガイドブックは，個人情報を取り扱う企業にとっての注意義務の指標となると解すべきである。

そして，前記(1)ア㈠ないし㈤のとおり，安全対策基準には，「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」との，内部不正防止ガイドラインには，「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」との記載がそれぞれあり，データセンターセキュリティガイドブックには，ＵＳＢメモリ等の情報記憶媒体や携帯電話の持ち込み・持ち出し制限がセキュリティ対策として挙げられていた。

また，シンフォームの業務用パソコン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り，業務用アカウントを教示されている従業者であれば，容易に顧客情報にアクセスすることが

可能な状況であったから，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に書き出しさせるような事態が万が一にも起きないように細心の注意を払うべきであった。

さらに，私物の持ち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防止対策である。

これらに照らせば，シンフォームは，再委託先を含めた従業員による私物スマートフォンの執務室への持ち込みを禁止する措置を講ずべき注意義務があった。

しかし，シンフォームは，再委託先を含めた従業員による執務室への私物スマートフォンの持ち込みを禁止せず，漫然と，大量の個人情報を取り扱う現場に持ち込むことを許容していたものであるから，本件漏えいについて過失があった。

イ　ＵＳＢ接続に係る注意義務違反

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，…外部記録媒体を接続できないようにする）」ことが望ましい措置であると規定されているところ，経済産業分野ガイドラインで「望ましい」と記載されている規定について，当該事業者の企業規模，取り扱う個人情報の量や内容いかんによっては，その規定に違反すれば，個人情報保護法には違反しなくとも，私法上の注意義務違反になり得るというべきである。

また，内部不正防止ガイドラインは，個人の情報機器及び記録媒体を持ち込まれた場合の情報持ち出しのリスク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たところ，前記アのとおり，内部不正防止ガイドラインで要求する事項が考慮されていない場合には，注意義務違反があったと解すべきである。

さらに，マネジメントシステム実施ガイドラインには，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，業務上の必要性に基づく限定対策として掲げられていたところ，マネジメントシステム実施ガイドラインは，ＪＩＳＱ１５００１により個人情報保護マネジメントシステムを構築し，運用するためのガイドラインであるから，これらで要求されている事項を満たさない場合には，業務上個人情報を取り扱う事業者に要求される水準に達しないものとして，注意義務違反と解すべきである。

また，業務用アカウントを教示されている従業者であれば，容易に顧客情報にアクセスできる状況にあったことからすれば，シンフォームとしては，アクセスした顧客情報がスマートフォン等に書き出される事態が万が一にも起きないよう，細心の注意を払うべきであった。

そして，ＵＳＢ接続口を物理的に壅塞する器具は，遅くとも平成１７年には発売されており，情報漏えい対策として古典的で一般的なものであって，機密情報を扱う部署において，通常，パソコンのＵＳＢ接続が物理的にできることはほとんどない。現に，千葉県袖ケ浦市で，平成２０年，ＵＳＢ接続口を物理的に壅塞する方法が検討されていた。

さらに，ＵＳＢ接続口を物理的に壅塞したり，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対策である。

これらに照らせば，シンフォームは，執務室において，業務用パソコンのＵＳＢポートに対する接続を禁止する措置を講ずべき注意義務があった。

しかし，シンフォームは，ＵＳＢ接続口を物理的に壅塞する措置も執らず，日常的にスマートフォン等が業務用パソコンにＵＳＢケーブルで接続されていたにもかかわらず，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ものであるから，シンフォームには，本件漏えいについ

て過失があった。

ウ　書き出し制御に係る注意義務違反

シンフォームが，セキュリティソフトにより，ＭＴＰでデータを転送するデバイスを業務用パソコンで使用できないようにするなど，業務用パソコンからデバイスへのデータの書き出しを制御する措置を講じていれば，本件漏えいを回避することができたところ，ＭＴＰ接続は，ごく一部の専門家が研究レベルで使用していた時点ではともかく，同接続が可能な端末が商品化されて一般の市場に出回った時点では，誰でも容易に同接続を利用することが可能になったのであるから，仮に同接続が可能な端末のスマートフォン市場におけるシェアが低かったとしても，その時点でセキュリティ上の対策をすべき注意義務があった。

なお，平成２４年夏以降に発売された「Ａｎｄｒｏｉｄ」をＯＳとするスマートフォン端末は，全て「Ａｎｄｒｏｉｄ４．０」以降のＭＴＰ対応端末であり，相当程度市場に出回る（出荷される）見通しであったから，それを予測できる時点で，その対策が当然に必要となるというべきであり，平成２６年まで何らの対策も採らなかったことが正当化される根拠とはなり得ない。

被控訴人らが導入していたセキュリティソフトにおいては，ＭＴＰをデータの転送に使用するデバイスであるＷｉｎｄｏｗｓポータブルデバイス（以下「ＷＰＤ」という。）を使用禁止とすることが可能であったのであるから，これにより，業務用パソコンから本件スマートフォンへのＭＴＰによるデータの書き出しを制御することができたのであり，このような措置を講じていなかったシンフォームには注意義務違反がある。

エ　アラートシステムに係る注意義務違反

シンフォームは，私物スマートフォン等の持ち込み禁止措置及び業務用パソコンに対するＵＳＢ接続禁止措置を採っていなかったのであるから，

業務用パソコンに接続した私物スマートフォン等の顧客情報を書き出す手法により，本件データベース上の大量の顧客情報が漏えいする可能性が常に存在していた。したがって，シンフォームには，本件データベースと業務用パソコンとの間に，通常業務における以上の通信量が認められた場合，それを許容するか否かを確認するアラートシステムを設置すべき注意義務があった。

このことは，被控訴人らが，本件漏えいの発覚直後から，再発防止策の緊急対策としてアラート機能を設定することを一番目の項目として挙げていたことや，被控訴人が，経済産業省への事故調査報告書において，アラートシステムが「機能しなかったため」，「不正行為等を防止することができませんでした」と記載したことからも明らかである。

しかし，シンフォームは，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パソコンとの間の通信量が一定の基準値を超えた場合に，当該パソコン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ものの，本件データベースのサーバについては，本格的運用開始前であったことを理由に，同システムを設定していなかったのであるから，シンフォームには，本件漏えいについて過失があった。

オ　監視カメラに係る注意義務違反

監視カメラで個人情報を取り扱う作業スペースを常時監視すれば，従業員による不正行為を抑止することができ，また，情報漏えいが起きた際にも速やかに対処することが可能であって，個人情報の拡散を抑制できるから，監視カメラの設置は，室内の不正行為を防止するために実効性がある。

また，シンフォームは，執務室を含む施設の主要な入退室口には防犯カメラを設置しており，監視カメラの設置は容易であった。

したがって，シンフォームには，個人情報の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注意義務があった。

しかし，シンフォームは，執務室を含む施設の主要な入退出口には防犯カメラを設置したものの，一番重要な執務室には監視カメラを設置しなかったのであるから，本件漏えいについて過失があった。

（被控訴人の主張）

(1) 本件漏えいの予見可能性について

通信方式がＭＴＰである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，通信方式がＭＴＰであるスマートフォンに対する（あるいは単に通信方式がＭＴＰの場合の）個人情報の書き出しのリスクについて，本件漏えいが発生するまで，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。

シンフォームとしては，外部記録媒体に情報を書き出すことを技術的に制限する高度なセキュリティソフトを導入していたため，執務室内の業務用パソコン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ところ，その業務用パソコンから外部記録媒体に書き出しがされ外部に情報が持ち出された等の外部記録媒体に対する書き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，充電のため業務用パソコン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き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き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。

(2) スマートフォンの持ち込み禁止に係る注意義務違反について

ア　安全対策基準

安全対策基準は，そもそも現在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，シンフォームの注意義務の根拠たり得ない。

また，安全対策基準中の控訴人指摘の「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また明らかである。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，控訴人が，情報システム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ち込み禁止措置を義務付けるものではない。

イ　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「サーバルーム」のみを対象としてその持ち込み・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ち込み禁止措置を義務付けるも

のではない。

ウ　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，被控訴人ら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ち込み禁止措置を義務付けるものではない。

エ　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他のガイドラインには，スマートフォンの持ち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得るとすれば，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ち込み禁止について，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ち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。

また，「私物スマートフォン等の持ち込み禁止」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ち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ち込み禁止は，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いわざるを得ない。

(3) ＵＳＢ接続に係る注意義務違反について

ア　経済産業分野ガイドライン

本件漏えい当時，業務用パソコンに対するＵＳＢ接続禁止措置については，経済産業分野ガイドラインでは，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，Wの使用する業務用パソコンはかかる端末ではなかった。

イ　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」を業務用パソコン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，業務用パソコンに対するＵＳＢ接続禁止措置を義務付けるものではない。

ウ　マネジメントシステム実施ガイドライン

ＪＩＳＱ１５００１及び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。

エ　その他

本件漏えい当時，業務用パソコンに対する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

ュリティ対策を採っている会社は数％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採っていないのであるから，業務用パソコンに対するＵＳＢ接続禁止は標準的な措置であったとはいえない。

また，ＵＳＢ接続口を物理的に塞塞する器具は取り外し可能であり，パソコンには，マウスやキーボード，業務上利用されるＵＳＢ（シンフォームの場合であれば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接続口が必要であって，全てのＵＳＢ接続口を塞塞できないから，結局のところ，ＵＳＢ接続口（余分な接続口）を物理的に塞塞することは，内部悪意による個人情報の漏えいに対する有効な対策とはならない。

(4) 書き出し制御に係る注意義務違反について

ア　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(2)イのとおり，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，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，個人情報機器及び記憶媒体の業務利用及び持ち込みの制限であって，情報書き出し制御措置については記載されていない。

イ　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，書き出し制御措置について記載されていない。

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，書き出し制御措置を採っていないものが過半であり，書き出し制御措置は，標準的なセキュリティ対策にはなっていなかった。

なお，シンフォームは，平成１７年から，その業務用パソコンに導入していたセキュリティソフトにより，書き出し制御措置を採用していたところ，本件漏えい当時，通信方式がＭＴＰであるスマートフォンに対しては有効に書き出しを制御することはできなかったものの，その余のスマートフォンについては，当該制御措置により，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）やライティングソフトによるＣＤ及びＤＶＤへの書き込みを禁止することができた。

ウ　控訴人は，被控訴人らが導入していたセキュリティソフトにおいては，ＷＰＤについて使用禁止とすることが可能であり，これによりＭＴＰによる書き出しを制御することできたと主張するが，ＭＴＰを使用する機器として念頭に置かれていたのは，デジタルカメラや携帯音楽プレイヤーなど，情報漏えいのリスクと考えられていなかった機器であり，これらのデバイスであるＷＰＤを使用禁止にしなかったことは，被控訴人の義務違反を構成するものではない。ＭＴＰに対応したスマートフォンによる情報漏えいのリスクは，本件事故に至るまで情報セキュリティの専門家ですら気づいていなかったものであり，このような状況で，シンフォームにおいて，セキュリティソフトでＭＴＰによる通信を制御する義務を負うと解することはできない。

(5) アラートシステムに係る注意義務違反について

ア　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(2)イ及び(4)アのとおり，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，シンフォームの注意義務の根拠たり得ない。

イ　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。

ウ　その他

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，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，その理由いかん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。

(6) 監視カメラに係る注意義務違反について

ア　ガイドライン等について

㈠ 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(2)イ，(4)ア及び(5)アのとおり，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，シンフォームの注意義務の根拠たり得ないし，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。

㈡ データセンターセキュリティガイドブック

控訴人が，データセンターセキュリティガイドブックのどの部分に記載されている記述を指して，「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）が挙げられている」旨主張しているのかは定かではない。データセンターセキュリティガイドブック５０頁では

「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に言及していたが，これは（敷地区画で用いられる画像監視システムと異なる点として）「証跡としての役割を果たすことが挙げられます」とされており，１００頁から１０３頁で紹介されている「画像監視システム」は，侵入者や不正行為の監視・記録を目的とするものであり，いずれも，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　その他

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，従業員が業務用パソコン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，業務用パソコン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，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，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。

情報セキュリティの考え方の基本は，ありとあらゆる方策の中から，当該企業に合った形で，対策としての実効性，コスト，業務阻害性その他諸般の事情を考慮して，具体的対策を選択実施するというものであるところ，執務室内へ監視カメラを設置することによっても本件漏えいのような態様により個人情報が不正に取得される事故を防ぐことはできず，実際，シンフォームにおいても，執務室内へ監視カメラを設置していたにもかかわらず本件漏えいが発生したのであって，この点についてシンフォームに過失はない。

(7) まとめ

シンフォームの情報セキュリティ対策は，外部脅威及び内部脅威（内部過失と内部悪意）の全てを想定したうえで，それぞれの脅威について適切な形で階層的に対策が講じられており，また，通常考えられるいずれの階層でもシンフォームの業務等に照らして適切と考えられる具体的対策を選択して，十分な対策が採られていたのであって，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国内企業，すなわち製造業，流通・ＥＣ（インターネット通信販売），更には金融業も含め，当該業界において大手ないし代表的と目される企業との比較においても遜色ないものであったから，シンフォームには，本件漏えいについて過失はない。

2　本件漏えいについて被控訴人に過失があったか否か（争点２）

（控訴人の主張）

(1) 本件漏えいの予見可能性

被控訴人が，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ことは，前記１（控訴人の主張）(1)と同様であ

る。

(2) 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，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った（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係る注意義務違反

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恐れがあり，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当たって，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，本件業務を別会社であるシン

フォームに委ね，シンフォームが同業務の一部を更に第三者に委託し，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，シンフォームに対する適切な監督を妨げ，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ち込みに係る注意義務違反等

被控訴人は，本件データベースに関するシステム開発・運用をシンフォームに委託していたものの，元々が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，シンフォーム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，実質的には，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ものであるから，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の開発・運用を行い，組織的に一体として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，シンフォームと同様の注意義務，すなわち，前記１（控訴人の主張）(2)のとおり，私物スマートフォンの持ち込み禁止措置義務，業務用パソコンに対するＵＳＢ接続禁止措置義務，情報書き出し制御措置義務，アラートシステム設定義務及び監視カメラの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　委託先選任及び監督に係る注意義務違反

被控訴人は，本件データベースの開発・運用や保守管理を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，被控訴人は，個人情報保護法上，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。

この点，委託契約の中に個人情報保護法２０条に基づく安全管理措置を講ずる受託者の義務を盛り込むことだけで「必要かつ適切な監督」を行ったことにはならず，契約内容の遵守について定期的に報告を受けたり，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る場合には，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を監督することも，同法２２条に基づく個人情報取扱事業者の監督責任に含まれる。

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定しなければならない。このため，事業者は，委託を受ける者を選定する基準を確立しなければな

らない。」，「事業者は，個人情報の取扱いの全部又は一部を委託する場合は，委託する個人情報の安全管理が図られるよう，委託を受けた者に対する必要，かつ，適切な監督を行わなければならない。」，「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」等を例示していた。

これに，前記アのとおり，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，①業務委託先を選任するに当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，②個人情報保護法２０条の安全管理措置が委託先で適切に採られているかを監督する義務を負っていた。

しかし，被控訴人は，シンフォームが，前記１（控訴人の主張）(2)のとおり，本来，私物スマートフォン等の持ち込み禁止措置，業務用パソコンに対するＵＳＢ接続禁止措置，情報書き出し制御措置，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，又は少なくとも過失によりかかる体制を把握せずに委託先にシンフォームを選任した。

また，被控訴人は，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，シンフォームによる被控訴人の顧客情報の具体的な取扱状況について正確に把握していなかった。とりわけ，アラートシステムに関しては，その対象範囲を委託先監査の対象としていなかった。そのため，被控訴人は，シンフォームにおいて，私物スマートフォンの持ち込み禁止措置，業務用パソコンに対するＵＳＢ接続禁止措置，情報書き出し制御措置がされておらず，アラートシステムの対象範囲の設定が適正に行われておらず，執務室の監視もされていないことを把握せず，仮に把握していたとしても，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。

（被控訴人の主張）

(1) 本件漏えいの予見可能性について

委託元である被控訴人は，本件漏えい当時，「シンフォームにおいて，開発及び運用業務に従事し正規のアクセス権限を有していたWが，その所有する特定の機種のスマートフォンをクライアントパソコンにＵＳＢケーブルにて接続することによりクライアントパソコンからスマートフォンにデータを転送する方法によって，個人情報を不正に取得すること」を具体的に予見しておらず，また具体的に予見し得なかった。

(2) 個人情報の利用・管理に責任を持つ部門設置に係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，それを設置しなかったことが第三者（顧客等）に対する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，飽くまで望ましい手法にとどまる。）。

さらに，控訴人は，被控訴人が顧客情報の利用・管理に責任を持つ部門を設置しないことによって，シンフォームに対する適切な監督を妨げ，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と主張するが，具体的な因果の流れが全く主張されておらず，主張として不特定・不十分である。

なお，控訴人が不十分であったとするシンフォームの情報管理体制の具体的内容が不明確であるが，その採っていた情報セキュリティ対策が標準以上のものであったことは，前記１（被控訴人の主張）(2)ないし(7)のとおりであり，シンフォームにおける情報セキュリティに関する統括責任者及び部署等が明確に定められて組織的な管理体制も十分であったことからすると，この点について控訴人が主張する義務違反と本件漏えいとの間に因果関係はない。

(3) 私物スマートフォンの持ち込みに係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ことは，我が国の法の基本であり，例外的に，厳格な要件のもと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すぎない。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，被控訴人がシンフォームと同様に注意義務を負うということはできない。したがって，この点に関する控訴人の主張は

失当である。

(4) 委託先選任及び監督に係る注意義務違反について

ア　前記１（被控訴人の主張）(2)ないし(6)のとおり，そもそも，シンフォームにおいて，控訴人が主張する上記各措置を講じる義務は存在しなかったから，シンフォームがかかる措置を講じ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が認められるはずがない。

イ　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，社会的に高い情報セキュリティ管理レベルを期待される，製造，流通・ＥＣ，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，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，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，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，シンフォームは，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。

ウ　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，シンフォームに対する委託先監督を実施していた。

被控訴人らは，インターネットプライバシー研究所に対し，被控訴人が本件漏えい当時実施していたシンフォームに対する委託先監督が，当時の

経済産業分野ガイドラインの「２－２－３－４．委託先の監督（法第２２条関連）」に適合していたかどうかの調査を依頼したところ，同研究所は，平成２８年１月から４月にかけて調査を行い，その結果，被控訴人が平成２６年当時実施していたシンフォームに対する委託先監督は，上記ガイドライン「２－２－３－４．委託先の監督」部分のいずれの項目についても，望ましいとされていた事項まで全て網羅して実践されていたことを確認している。

３　シンフォームは，Wによる本件漏えいについて使用者責任を負うか否か（争点３）

（控訴人の主張）

(1) シンフォームの使用者性

民法７１５条の使用者責任の根拠は，自己の利益のために被用者に事務を処理させる使用者には，被用者の行為によって他人に与えた損害についても責任を負わせることが公平であること（いわゆる報償責任）に求められることから，使用関係の有無を判断するに当たっては，使用者責任の根拠に鑑み，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，シンフォームとWの間に直接の雇用関係はないが，Wは，システムエンジニアとしてシンフォームに派遣され，シンフォーム多摩事業所で本件業務等に従事し，日常的にシンフォームの社員から指示を受けていた。シンフォームは，Wに対し，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，業務用パソコンを貸与し，業務開始時の入館証発行に当たっては研修を受けさせ，それ以降，毎年研修を実施していた。

このような具体的な事情からすれば，シンフォームは，本件システムに関する事業について，W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。

(2) 事業執行性

Wによる本件漏えいは，被控訴人からシンフォームが委託を受けた本件業務を，シンフォーム多摩事務所においてWが行っている際にされたものであるが，W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，シンフォームの「事業の執行」に該当する。

(3) 以上より，シンフォームは，Wによる本件漏えいについて使用者責任を負うものである。

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）

(1) シンフォームの使用者性について

シンフォームと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，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，W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，シンフォームは，Wを実質的に指揮監督する関係にはなかった。

なお，シンフォームにとってWは個人情報保護法２１条の従業者に当たるとの控訴人の主張が誤りであることは明らかである。

(2) 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。W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，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，控訴人は，W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，そもそもシンフォームの事業ではあり得ないし，Wの職務の範囲内であることもおよそ考えられない。

(3) 選任監督上の相当の注意をしていたこと

本件において，シンフォームは，①W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，②W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。このような事情に鑑みれば，シンフォームは，同社とW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というべきである。

4　被控訴人は，シンフォームの不法行為について使用者責任を負うか否か（争点４）

（控訴人の主張）

(1) 被控訴人の使用者性

前記３（控訴人の主張）(1)記載のとおり，使用関係の有無は，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ところ，以下の事情からすれば，被控訴人は，本件システムに関する事業について，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。

ア　被控訴人とシンフォームとの間の業務委託契約では，被控訴人が，被控訴人における安全管理措置と同等の措置がシンフォームにおいて講じられるように監督することや，シンフォームが受託業務を再委託する場合には，事前に被控訴人の承諾を求めることとされていた。また，同契約は，被控

訴人の販促活動のために，顧客情報を統合して分析に使用するための本件システムを構築する業務を，被控訴人がシンフォームに委託したというものであり，かかる業務委託契約の趣旨からして，当然，本件システムの具体的内容の決定権限は被控訴人にあった。

イ　被控訴人は，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うとともに，月次で「アウトソーシングレポート報告会」を開催して委託業務全般の進捗状況の確認を行い，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。

ウ　被控訴人は，本件データベースの運用に当たり，動作状況を確認し，シンフォーム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。

エ　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，説明会を実施してシンフォーム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，その都度シンフォームのセキュリティの設定状況を確認していた。

オ　被控訴人とシンフォームとは，現在は，ベネッセホールディングスの１００％子会社同士の兄弟会社の関係にあるが，もともと，シンフォームは，被控訴人の１００％子会社であったものであり，その当時から本件漏えいが発生するまで，被控訴人の指示の下，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，同社の取締役又は監査役がシンフォームの役員に就任するなど，ベネッセグループとしてシンフォームと一体で事業を行っていた。

カ　被控訴人は，シンフォームに本件システムを構築させるに当たり，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訴外Ｚ氏に，平成２５年１月から平成２６年３月までシンフォームのＩＴソリューション部の部長を兼務させていた。

キ　被控訴人は，本件データベースの運用に当たり，動作状況を確認し，シンフォーム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。すなわち，本件システムの最終的な動作確認権限が被控訴人にあった。

ク　被控訴人は，委託業務全般の進捗状況の確認を行っていた。

(2) 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るから，その構築業務，開発及び運用は，被控訴人の「事業の執行」に該当する。

(3) 以上より，被控訴人は，シンフォームの不法行為について使用者責任を負うものである。

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）

(1) 被控訴人の使用者性

控訴人が，被控訴人においてシンフォームを実質的に指揮監督していたことを根拠付ける事情として指摘する点は，いずれも，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り，委託元として委託業務の進捗を確認したり，個人情報保護のための情報提供や監督を行ったりしたものにすぎず，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。

なお，シンフォームと被控訴人は独立した法人であり，事業遂行も独自に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。

(2) 事業執行性について

控訴人は，シンフォームの行為が被控訴人の事業の範囲内に属していたことのほか，シンフォームの行為が同社の被控訴人における「職務」の範囲に属していたことを主張立証すべきであるところ（最三小判平成２２年３月３

０日集民２３３号３７３頁等参照），控訴人の主張は後者を全く欠いており，主張として失当である。

また，仮に前記（控訴人の主張）(2)のような理由で事業執行性が肯定されるとすれば，ある会社が別の会社の事業に用いるための業務を何らか受託した場合には，当然に，受託会社がその契約に基づき行う業務が委託元の「事業の執行」に該当することとなり，極めて奇妙であるといわざるを得ない。

(3) 選任監督上の相当の注意をしていたこと

仮に本件におけるような委託先との関係で使用関係が認められるとするならば，その選任及び監督の判断に当たっては，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での判断がされるべきである。

そして，被控訴人は，シンフォームの選任及び監督に当たって，個人情報保護法上求められる義務を尽くしていた以上，民法７１５条が定める選任及び監督の注意も尽くしていたといえる。

5　被控訴人らの共同不法行為責任の有無（争点５）

（控訴人の主張）

シンフォームは，被控訴人の保有する個人情報の管理を受託していたのであるから，被控訴人らは，控訴人らを含む個人情報の情報主体に対し，共同で安全管理措置を徹底する注意義務を負っていたのであり，被控訴人らがかかる注意義務を怠ったことは，共同不法行為となる。

（被控訴人の主張）

争う。

6　控訴人の権利侵害の有無（争点６）

（控訴人の主張）

(1) Wの本件漏えいにより，以下のとおり，控訴人らの個人情報が漏えいした。

ア　控訴人の情報　　氏名，性別，生年月日及びメールアドレス

イ　選定者Ｂの情報　　氏名，性別，生年月日及びメールアドレス

ウ　選定者Ｃの情報　　氏名，性別，生年月日及び続柄〔子〕

エ　控訴人ら共通の情報　郵便番号，住所，電話番号

(2) 漏えいした上記の個人情報は，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，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極めて慎重な取扱いが求められる家族関係の情報も一定程度明らかとなる。

それればかりか，漏えいした個人情報により，控訴人らが，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されてしまっている（だからこそ，通信教育を手掛ける株式会社ジャストシステムが当該名簿を買ったものである。）。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，控訴人らにとっては，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。

また，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ところ，かかる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，基本情報の流出にす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。

したがって，本件漏えいの結果，本件個人情報が名簿業者等に漏えいしたことが，控訴人らのプライバシー侵害に当たることは明らかであり，違法性が認められることも明らかである。

（被控訴人の主張）

(1) 本件漏えいにより流出したと控訴人らが主張する本件個人情報のうち，続柄〔子〕については否認し，その余は認める。ただし，受領した情報の真実性については個別に確認しているわけではない。

(2) 本件における諸事情（本件個人情報の内容・性質，開示された対象，範囲，それにより予想される利用方法，控訴人への影響，開示行為により控訴人が被った具体的な不利益の内容，程度〔実質的不利益〕，被控訴人らの行為の態様，程度，本件漏えい後の被控訴人らの対応，本件漏えいによる被控訴人らへの影響ないし被害，仮に被控訴人らに賠償義務があるとした場合，本件における影響，今後の同種事件における影響等）を丹念にみてそれを総合考慮したとしても，また，最高裁平成１４年（受）第１６５６号平成１５年９月１２日第二小法廷判決・民集５７巻８号９７３頁（以下「早稲田大学江沢民事件」という。）との対比においても，本件での被控訴人らの行為が，社会通念上許容される限度を逸脱した違法な行為であるとみる余地はない。

７　控訴人らの損害の有無及びその額（争点７）

（控訴人の主張）

被控訴人ら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，控訴人らは，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。また，本件個人情報には，未成年者の情報も含まれていることから，選定者Ｃ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。さらに，本件個人情報は，続柄や電話番号にも及ぶため，いわゆるオ

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できるから，控訴人らの不安感は重大であるし，子供の情報を含むため，その不安感は長期間継続することになる。

したがって，かかる精神的苦痛を慰謝するには，控訴人及び選定者Ｂについて５万円が，選定者Ｃについて１０万円がそれぞれ相当である。

（被控訴人の主張）

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，かかる勧誘等は日常ごくありふれた行為で，一般に許容されており，それによって，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。住所，氏名及び電話番号等の個人情報の名簿業者への流出は，それにより営業や宣伝に係る郵便物が増加し，架電されることはあり得るが，些細な不快があったとしても日常あり得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や不安であって，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価すべきものである。

本件は，早稲田大学江沢民事件において問題となった情報よりもその秘匿性は低く，かつ，その開示相手や予想される利用形態等に照らして，控訴人の感じる不安感や不快感などの精神的負担も低いものである上，被控訴人らが故意に本件個人情報を開示したものではなく，被控訴人らに対する非難の印として損害を認定する必要性も全く認められないのであるから，控訴人の精神的損害の発生は認められず，仮にそれがあるとしてもその程度は著しく低いものであって，一般的平均的な人の感性を基準として，慰謝料の支払を受けるべき程度のものとは到底いえない。

また，本件漏えい後，被控訴人らを含むベネッセグループは，被控訴人を中心として，本件漏えいに対応したものであり，これらの対応は，控訴人の精神

的損害が仮にあったとしてもそれを慰撫するのに十分なものであって，現時点において，控訴人に慰謝すべき精神的損害があるとはいえない。

なお，従来，不法行為法の目的は，被害者救済，損害の填補及び加害者と被害者の公平の実現などといわれてきた。しかし，被害者に具体的な損害の発生がなく，抽象的で漠然とした不安感，不快感等を内容とする精神的損害が主張されている事案では，損害賠償は，上記目的と直ちに結びつくものではない。また，不法行為法の目的として，これらのもののほか，新たに，加害行為の抑止及び制裁や被害者の権利保護の観点を考慮する余地もあり得なくはないと思われるが，本件ではこれも妥当しない。本件は，故意による開示ではなく，被控訴人らとしては顧客等の個人情報保護のため十分なセキュリティ措置を講じていたにもかかわらず情報が持ち出されてしまったものであるから，加害行為の抑止及び制裁の効果を果たさせるため被害者への賠償を認める必要もなく，また，被控訴人らとして本件漏えいを重大に受け止めて真摯に対応してきていることからすると，被害者の権利保護の観点から本件を違法と宣言する効果を重視して被害者への賠償を認める必要もない。むしろ，被控訴人に損害賠償を命じることは，仮にそれが，早稲田大学江沢民事件の差戻審判決が認定したのと同じ５０００円であったとしても，それは被控訴人にとって，名目的であることは全くなく，被控訴人らの命運を絶つ可能性もあるのであって，余りに過酷な制裁を加えるものとなる。

第５　当裁判所の判断

１　争点１（本件漏えいについて，シンフォームに過失があったか否か）について

(1) 本件漏えいの予見可能性について

ア　前記前提事実，後掲の証拠及び弁論の全趣旨によれば，次の事実が認められる

㈠　ＭＴＰ・ＭＳＣなどについて

本件スマートフォンは，ＭＴＰに対応していたが，当時，スマートフォンなどのデバイスをＵＳＢケーブルでパソコンに接続してデータの転送を行う規格には，他にＭＳＣ（ＵＳＢマスストレージクラス〔Ｍａｓｓ　Ｓｔｒａｇｅ　Ｃｌａｓｓ〕の略。パソコンとデバイスの接続に用いられる規格。以下「ＭＳＣ」という。）があった。

ＭＴＰでもＭＳＣでも，パソコンにスマートフォンなどのデバイスをＵＳＢケーブルで接続してデータの転送をすることが可能である点で違いはない。ＭＳＣでは，ファイルシステムの管理などはパソコン側のＯＳで行われ，接続されたデバイスは，ＵＳＢに接続された外部記憶装置（ＵＳＢメモリや外付けＨＤＤなど）と同等に管理・利用される。これに対し，ＭＴＰは，デジタルカメラの画像転送プロトコル（ＰＴＰ）をベースに，音楽・動画ファイルなどの転送を可能にした規格であり，デジタルオーディオプレイヤーやデジタルメディアプレイヤーに音楽ファイルや動画ファイルを転送する目的で設計され，これらのプレイヤー等に採用されており，ファイルシステムの管理などはデバイス側で行われるという違いがある。そして，接続されたデバイスは，ＷＰＤなどとしてパソコン側のＯＳであるＷｉｎｄｏｗｓには認識される。

Ｗｉｎｄｏｗｓの場合，ＯＳ自体がＭＴＰに対応しているので，デバイスドライバや対応するアプリケーションをインストールすることなしに，ＭＴＰに対応するデバイスにデータを転送することが可能であった。（甲１１，１０２，乙９９，１０２ないし１０４）

㈠　被控訴人らが導入していたセキュリティソフトについて

被控訴人らが，業務用パソコンに導入していたセキュリティソフトは，株式会社日立ソリューションズ製であった（以下「本件セキュリティソフト」という。）。平成２３年７月ころには，本件セキュリティソフトによって，リムーバブルメディア，ＣＤ／ＤＶＤ，外付けＨＤＤのほか，

終端機器としてイメージングデバイス，ＷＰＤ，その他制御デバイス等，通信機器として無線ＬＡＮ，モデム，赤外線等について使用可否制御が可能となっていた。そして，これらのデバイスの全てを制御して使用を禁止した場合，ＰＣからのデータの書き出しは不可能であった。

本件セキュリティソフトにおいては，リムーバブルメディア，ＣＤ／ＤＶＤ，外付けＨＤＤについては，データの書き出しを禁止できる書き出し制御が可能であり，リムーバブルメディアについては，組織で管理していないＵＳＢメモリのデータの読み書きを禁止できるＵＳＢメモリの個体識別制御が可能であった。また，読み書きを個別に許可されたＵＳＢメモリについては，書き出されたデータは暗号化された。

被控訴人らは，本件セキュリティソフトで，書き出し制御が行われているリムーバブルメディア，ＣＤ／ＤＶＤ，外付けＨＤＤ以外は，全てのＵＳＢデバイスが使用禁止されていると考えていたが，実際には，リムーバブルメディア，ＣＤ／ＤＶＤ，外付けＨＤＤだけが書き出し制御の対象とされ，データの書き出しが禁止とされる設定になっていた。

個々のデバイスの制御は，自由に変更することが可能であり，作業手順さえ踏めばシンフォームにおいて自由に変更することができた。平成２３年８月にシンフォームに納品された本件セキュリティソフトのパラメータシートには，「デバイス制御設定」欄の「①デバイス使用可否制御を有効にする，②デバイス個体識別制御を有効にする，③個体識別ログの出力を有効にする」の３つの項目のチェック欄にチェックがされておらず，設定がされていないことが表示されていた。

スマートフォンは，Ｗｉｎｄｏｗｓにおいて，リムーバブルメディア，ＷＰＤ，イメージングデバイス，その他制御デバイスのいずれかで認識されるが，本件漏えい当時の本件セキュリティソフトの設定では，スマートフォンがリムーバブルメディアとして認識される場合（データの転

送にＭＳＣを使用する場合）にのみ，書き出し制御の対象となるが，本件スマートフォンのようにデータの転送にＭＴＰを使用しＷＰＤで認識される場合は，デバイスの使用は許可されており，書き出されたデータの暗号化もされなかった。

シンフォームは，本件漏えい後に，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日以後は，リムーバブルメディア，ＣＤ／ＤＶＤ，外付けＨＤＤについて従前どおりデータの書き込みを禁止し，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を，使用可否制御により使用禁止とし，上記パラメータシートの「①デバイス使用可否制御を有効にする，②デバイス個体識別制御を有効にする，③個体識別ログの出力を有効にする」の３つの項目のチェック欄にチェックを入れた。（甲７３，７７ないし７９）

㈣　Ｗによる本件漏えいについて

Ｗは，本件漏えい当時，経済的な苦境状態にあり，本件業務で扱っている被控訴人の顧客情報を名簿業者に販売することを考えていたが，ＵＳＢメモリ等が書き出し制御の対象とされていることを認識していたので，これを諦めていた。そのような時に，Ｗは，本件スマートフォンを充電のために業務用パソコンに市販のＵＳＢケーブルで接続したところ，外部記憶媒体として認識され，業務用パソコンから本件スマートフォンにファイルを移動することができることを知った。そこで，Ｗは，被控訴人の顧客情報を書き出し，本件漏えいに及んだものであり，本件漏えいにおいて，ファイルの転送にはＭＴＰが使用された。（甲７１，８８）

イ　上記アの事実認定を踏まえ，本件漏えいに対する被控訴人らの予見可能性の有無について検討する。

㈠　本件漏えい以前から，一般的に，経済産業分野ガイドライン等（甲７，

９，１５）の中で，外部記憶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が，本件漏えいは，Wにおいて，通常想定できないような特別な知識や技術を使用して行われたものでないことは，上記のとおりである。当時において，スマートフォンをＵＳＢケーブルでパソコンと接続してデータのやり取りをすることが可能であることは，一般的に知られており，ＭＴＰも，データの転送に用いる規格として新規で特殊なものとはいえない。

㈠　本件では，本件スマートフォンが，従来使用していた規格であるＭＳＣではなく，それまで音楽ファイルや動画ファイルの転送を主な目的としてＯＳであるＷｉｎｄｏｗｓが対応していた規格であるＭＴＰに対応したために，データの転送が可能となったものである。デバイスやＯＳは，バージョンアップにより高機能化していくものであるから，それに応じて，接続されるデバイスを制御してデータの漏えいを防いでいく必要があるところ，被控訴人らは，本件セキュリティソフトを導入していたことに照らすと，このような必要性を具体的に認識していたと認めるのが相当である。

㈡　以上によれば，被控訴人らには，ＭＴＰ対応の本件スマートフォンを使用した本件漏えいについて，予見可能性があったというべきである。

ウ　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商用デバイス制御ソフトのうちＭＴＰ使用制限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と主張するので，以下検討する。

㈠　本件漏えい当時のＭＴＰ対応スマートフォンの国内シェアについて

確かに，「携帯電話端末におけるＭＴＰ普及率についての調査報告」（乙３６）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，５９３万台余りということになる。

しかしながら，仮に上記の報告のとおりであったとしても，ＭＴＰ対応のスマートフォンは，平成２４年頃から急速に普及してきていたこと，本件漏えい当時において，多数のＭＴＰ対応のスマートフォンが市中に出回るようになっていたことなどが認められる。そうすると，本件漏えい当時のＭＴＰ対応スマートフォンの国内シェアに関する上記報告によって，ＭＴＰに対応するスマートフォンを使用した本件漏えいについて，被控訴人らに予見可能性があったことを認める上記判断を覆すことはできないというべきである。

(イ) 本件漏えい当時の商用デバイス制御ソフトにおけるＭＴＰ制御機能への対応について

確かに，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（シンフォーム３７）には，平成２６年６月当時販売されていた主要な端末管理・セキュリティ製品について，実用的なＭＴＰ制御機能は，国内市場シェアが高い製品については全く搭載されておらず，実用的なＭＴＰ制御機能を搭載していたと認められる製品は，国内市場シェアが微少な１製品にとどまり，かつ，初期設定ではＭＴＰ制御機能は無効とされていた旨の記載がある。しかし，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パソコンにデータを転送することは可能であるが，パソコンからリムーバブルメディアにデータを転送することは不可能とする設定）ができる場合」と定義し，「実用的」でない製品についてはＭＴＰ制御機能を搭載していないものとして扱っているところ，前記(1)ア㈠のとおり，被控訴人らが導入していた本件セキュリティソフトは，ＭＴＰに対応するデバイスについて，使用可否制御により使用禁止することが可能であった。そうすると，上記の定義は，被控訴人らが導入していた本件セキュリティソフトをもＭＴＰ制御機能を搭載しないものとして扱うものであるから，相当とはいい難く，上記報告は，報告書としてその前提を誤ったものと評価せざるを得ない。

㈢　スマートフォンを利用した個人情報不正取得の危険性の認識について

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，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く，本件漏えいの結果，そのような対策が追加されたことから，ＭＴＰ対応スマートフォンに対する対応をする注意義務は存在しなかったと主張するところ，この主張には，上記予見可能性もなかったとの主張も含まれていると解することができる。また，被控訴人は，特定非営利活動法人日本ネットワークセキュリティ協会で理事及び事務局長を務めるとともに一般社団法人日本スマートフォンセキュリティ協会で理事を務めるＵ氏の意見書（乙３４「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」）に基づき，本件漏えい前は一般に認識されていなかった脆弱性によって発生し，本件漏えいによって初めて，パソコンのリムーバブルメディアとして携帯電話（スマートフォンを含む。）が使用される危険性があることが認識され，セキュリティ業界がその対策を採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，ユーザーであるシンフォームが予見することは不可能であったと主張する。さらに，被控訴人は，情報セキュリティの専門家等の記事（乙３８，３９）を根拠に，本件漏えいの方法による情報漏えいの危険性を予見できなかったと主張する。

しかしながら，本件漏えいの以前にはＭＴＰ対応のスマートフォンを使用した情報漏えいの事例が報告されていなかったというだけで，その危険性について予見可能性がなかったといえるものではなく，上述したとおり，デバイスやＯＳは，バージョンアップにより高機能化していくものであるから，それに応じて，接続されるデバイスを制御してデータの漏えいを防いでいく必要がある。被控訴人らは，本件セキュリティソフトを導入していたことからして，このような必要性を具体的に認識していたものと認められ，また，本件漏えいは，一般的にいっても，特殊な知識や技術を用いた予見が困難なものではなく，むしろ，デバイスやＯＳの高機能化によって発生する危険の範囲内のものというべきであるから，予見可能性は否定されない。

エ　以上によれば，被控訴人らは，本件漏えい当時，本件漏えいと同様の方法で，本件個人情報が不正に取得されることを予見し得たというべきである。

そこで，以下，シンフォームが，控訴人の主張する各措置を講じなかったことについて，シンフォームの注意義務違反が認められるか，個別に検討する。

(2) スマートフォンの持ち込み禁止について

確かに，Wが執務を行う部屋に，私物のスマートフォンを持ち込むことを禁止する措置を採っていれば，本件漏えいを回避できたということができる。

しかし，個人情報等の情報を扱う以外にも通常の業務を行うような執務環境において，私物のスマートフォンの持ち込みを一切禁止するというのは，

当該執務環境において従事する者にとって，非常に大きな制約となることは明らかであり，加えて，後記(4)で説示するとおり，同様の効果を上げられる他の代替手段があり得ることに照らすと，シンフォームにおいて，本件漏えい当時，執務室内に私物のスマートフォンの持ち込み禁止措置を講ずべき注意義務があったということはできない。

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

ア　安全対策基準について

確かに，安全対策基準（甲１５）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とが認められる。

しかし，当該記載から，私物のスマートフォンを対象としているかどうか明らかとはいえない。かえって，安全対策基準が改正されたのは，平成９年が最後であるところ，同年当時，スマートフォンが市場で流通していたことを認めるに足りる証拠はないから，少なくとも，安全対策基準が具体的にスマートフォンを念頭に置いて策定されたとは考え難い。

そうすると，安全対策基準から，当然に私物のスマートフォンの執務室

内への持ち込みを禁止すべき注意義務があるとは認められない。

イ　内部不正防止ガイドラインについて

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

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

ウ　データセンターセキュリティガイドブック

確かに，データセンターセキュリティガイドブック（甲１０）では，共有区画として，オフィスとサーバー室に区別され，サーバー室については，脅威として情報の不正持ち出しの指摘があり，管理策として記録媒体の持ち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を根拠に，当然にスマートフォンの執務室内への持ち込み禁止措置を採るべき注意義務があるとは認められない。

したがって，この点に関する控訴人の主張は理由がない。

(3) ＵＳＢ接続禁止措置について

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

しかし，パソコンのＵＳＢポートは，外部記録媒体の接続以外にも，マウスを使用する際に用いるなど，業務上必要な装置を接続することが想定されている。控訴人は，マウスについて，ＵＳＢポートによる接続以外の方法での接続が可能であると主張するが，どのようなマウスであっても別の方法での接続が可能であると認めるに足りる証拠はなく，また，仮にその点をおくとしても，後記⑷で説示するとおり，同様の効果を上げられる他の代替手段があり得ることに照らすと，ＵＳＢポートを使用できなくするという措置は，スマートフォンの持ち込み禁止措置ほどではないにしても，業務に従事する者に対する制約として過度なものであるといわざるを得ない。

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

この点，控訴人は，①経済産業分野ガイドラインには，個人データを入力できる端末では，ＣＤ－Ｒ，ＵＳＢメモリ等の外部記録媒体を接続できない

ようにする旨の記載があること，②内部不正防止ガイドラインでは，個人の情報機器及び記録媒体を持ち込まれた場合の情報持ち出しのリスクや，外部記録媒体の業務利用を制限することを対策のポイントとして掲げていること，また，③マネジメントシステム実施ガイドラインでは，経済産業分野ガイドラインと同様の記載があることに照らすと，シンフォームには，本件漏えい当時，業務用パソコンのＵＳＢ接続の禁止措置を講ずべき注意義務があったと主張するので，以下検討する。

ア　経済産業分野ガイドラインについて

確かに，経済産業分野ガイドラインの平成２１年１０月版（甲７）には，個人データを入力できる端末では，ＣＤ－Ｒ，ＵＳＢメモリ等の外部記録媒体を接続できないようにするとの記載があるが，これは，望まれる事項の例の中で，「個人データを入力できる端末に付与する機能の，業務上の必要性に基づく限定」についての例示として挙げられているものにすぎないから，この記載をもって，当然に物理的にパソコンのＵＳＢポートを塞ぐ措置を講ずる注意義務があるということはできない。

イ　内部不正防止ガイドラインについて

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

ウ　マネジメントシステム実施ガイドラインについて

確かに，マネジメントシステム実施ガイドライン（甲２０）では，経済産業分野ガイドラインでの上記アの指摘と同様の指摘がされているが，上記アで説示したとおり，そのことから直ちにＵＳＢポートを塞ぐ措置を講

ずべき義務があるということはできない。

したがって，この点に関する控訴人の主張は理由がない。

(4) 書き出し制御措置について

前記(1)ア㈠のとおり，シンフォームにおいては，本件セキュリティソフトの使用可否制御により，ＭＴＰを使用するデバイスを使用禁止にしておけば，ＭＴＰ対応のスマートフォンによるデータの書き出しを防止することは可能であったことが認められる。また，被控訴人らは，本件セキュリティソフトにより，リムーバブルメディア，ＣＤ／ＤＶＤ，外付けＨＤＤのみが使用できると認識していたものであったほか，本件漏えい後に，本件セキュリティソフトの設定を見直し，リムーバブルメディア，ＣＤ／ＤＶＤ，外付けＨＤＤについて従前どおりデータの書き込みを禁止し，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を，使用可否制御により使用禁止としたものであるから，本件業務において，業務用パソコンについてＭＴＰを使用してデータの転送を行う必要性はなかったと認められる。

そうすると，本件において，ＭＴＰを使用するデバイスの使用が許可されていたのは，単にシンフォームにおいて，本件セキュリティソフトの設定の確認を失念ないし怠っていたことによるものというべきである。そして，シンフォームは，本件漏えいまでにＭＴＰ対応スマートフォンに対する書き出し制御措置を講ずることが可能であったから，そのような措置を講ずべき注意義務があったにもかかわらず，これを怠った点に過失があったと認めるのが相当である。

(5) アラートシステムについて

この点，前記第３の４(4)のとおり，シンフォームは，本件漏えい当時，連携システムについてはアラートシステムを設置していたことや，経済産業省の勧告（甲２３。以下「本件勧告」という。）でも，本件データベースに

ついてアラートシステムの対象となっていなかったことが指摘されていることからすれば，アラートシステムの設置が情報セキュリティの対策として必要であったことは否定できない。しかし，情報セキュリティ対策の中には，情報漏えい等の問題を事前に防ぐための対策から，何らかの問題が発生した場合に，その被害を最小限に食い止めるための対策まで，種々のものがあるところ，控訴人の主張するアラートシステムは，一定量の情報が一度に移動した際に，責任ある立場の者にアラート（警告）が送信され，当該状況に対してどのような対応をすべきかを判断する機会ができるというものであるから，情報漏えいを未然に防ぐことができるわけではない。また，どの程度の量の情報が移動した場合にアラートが発せられる設定とするかによって，それ以下の情報量であればアラートが発せられないことになり，必ずしも情報漏えいの全てを防ぐことができる対策ともいえない。

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

(6) 監視カメラについて

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

しかし，証拠（乙２９）によれば，本件漏えい当時，執務室内の全体的な状況を確認できる程度ではあるものの，シンフォームの執務室内に監視カメラが設置されていたことが認められるところ，それにもかかわらず本件漏えいを回避することができなかったものであるから，現に設置されていたものより高精度な監視カメラを設置したとしても，それによって本件漏えいを回避できたのかそもそも疑問であるといわざるを得ない。また，仮に，それをおくとしても，本件個人情報へのアクセス権限を有するWが，本件漏えいの

際に，監視カメラで確認することができ，かつ，通常の業務ではしないような行動をしていたのでない限り，現に設置されていたものより高精度な監視カメラの設置によっても本件漏えいを回避できたとは認められないところ，Wが，本件漏えいの際に，監視カメラで確認することができ，かつ，通常の業務ではしないような行動をしていたことを認めるに足りる証拠はない。

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

(7) 小括

以上のとおり，本件漏えい当時，シンフォームには，ＭＴＰ対応スマートフォンに対する書き出し制御措置を講ずべき注意義務があり，これを怠った過失があったと認められる。

2　争点２（本件漏えいについて被控訴人に過失があったか否か）について

(1) 本件漏えいの予見可能性

シンフォームだけでなく被控訴人にも，本件漏えいについて予見可能性があったと認められることは，前記１(1)で認定したとおりである。

そこで，以下，被控訴人が，控訴人の主張する各措置を講じなかったことについて，注意義務違反が認められるか否かを個別に検討する。

(2) 個人情報の利用・管理に責任を持つ部門設置に係る注意義務違反について

この点，証拠（甲７，１７，２３）によれば，経済産業分野ガイドラインにおいて，組織的安全管理措置の項目で，各項目を実践するために講じることが望まれる手法の例示として，「個人情報保護管理者（いわゆる，チーフ・プライバシー・オフィサー（ＣＰＯ））の設置」が挙げられているところ，被控訴人は，本件漏えい以前，同社の法令遵守状況を管理監督する機関としてコンプライアンス部を設け，コンプライアンス部長をＣＰＯ（最高個

人情報責任者）とし，その下に，専門部署として個人情報保護課を設置し，個人情報保護活動を行っていたこと，経済産業省は，被控訴人に対し，平成２６年９月２６日，同年１０月２４日までに個人情報保護法２０条に基づく安全管理措置及び同法２２条に基づく委託先の監督を徹底して，具体的な内容を報告するよう勧告（本件勧告）し，本件勧告の原因として，本件漏えいの対象となったデータベースが，個人情報のダウンロードを監視する情報システムの対象として設定されていなかったところ，被控訴人は，シンフォームに対して行う定期的な監査において，当該情報システムの対象範囲を監査の対象としていなかった等，委託先に対する必要かつ適切な監視を怠っていたことが同法２２条に違反し，被控訴人の業務の全過程においてシンフォームの保有する個人情報の利用・管理に責任を持つ部門を設置せず，その安全管理のために必要かつ適切な措置を講ずることを怠っていたことが同法２０条に違反する旨を指摘していることが認められる。

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

(3) 私物スマートフォンの持ち込みに係る注意義務違反等について

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

の一体性が認められると主張する。

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

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

(4) 委託先選任及び監督に係る注意義務違反について

ア　委託先選任に係る注意義務違反について

この点，被控訴人が，シンフォームを委託先として選任したことについて注意義務違反があったことを基礎付ける事実を認めるに足りる証拠はない。

被控訴人がシンフォームを委託先として選任したのは，平成２４年４月であり，前記１⑴のとおり，シンフォームが平成２３年７月に導入した本件セキュリティソフトの設定が適切でなかったという問題があることは認められるが，シンフォームは，機能的には本件漏えいを防止することの可能な本件セキュリティソフトを導入しているのであり，その設定が適切でなかったことをもって，委託業者として選任することが不適当であったということはできない。

したがって，この点に関する控訴人の主張は理由がない。

イ　監督に係る注意義務違反について

個人情報保護法２２条は，「個人情報取扱事業者は，個人データの取扱いの全部又は一部を委託する場合は，その取扱いを委託された個人データの安全管理が図られるよう，委託を受けた者に対する必要かつ適切な監督を行わなければならない。」と規定し，経済産業分野ガイドライン（甲７）

には，「必要かつ適切な監督」に関し，委託先を適切に選定すること，委託先に個人情報保護法２０条に基づく安全管理措置を遵守させるために必要な契約を締結すること，委託先における委託された個人データの取扱状況を把握することが含まれる旨の記載があり，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定しなければならない。このため，事業者は，委託を受ける者を選定する基準を確立しなければならない。」，「事業者は，個人情報の取扱いの全部又は一部を委託する場合は，委託する個人情報の安全管理が図られるよう，委託を受けた者に対する必要，かつ，適切な監督を行わなければならない。」等と規定し，マネジメントシステム実施ガイドラインは，「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」等を例示している（甲２０）ことに照らせば，大量の個人情報の運用管理をシンフォーム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監督をすべき注意義務があったところ，前記⑴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ものである。そして，前記１(4)のとおり，シンフォームにおいて，本件セキュリティソフトの設定を適切に行っていれば，本件漏えいは防止できたことが認められる。他方，被控訴人において，シンフォームに対し，ＭＴＰ対応スマートフォンに対する書き出し制御措置が講じられているか否かを確認すべく，本件セキュリティソフトの設定状況について適切に報告を求めていれば，ＭＴＰ対応スマートフォンに対する書き出し制御が十分でないことを知り，本件セキュリティソフトの使用可否制御を指示することができたと認められるところ，このような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は思われない。そうすると，被控訴人は，シンフォームが，本件セキュリティソフトの適切な設定を行っているか否かを監督する注意義務を負っていると解されるところ，被控訴人において本件セキュリティソフトについて適切な設定が行われていると誤信していたことにより，適切な監督を行うことができなかったものであるから，上記注意義務に違反した過失があると認めるのが相当である。なお，前記(2)のとおり，本件勧告においても，被控訴人が，シンフォームに対して行う定期的な監査の際に本件データベースを監査の対象としていなかった等，委託先に対する必要かつ適切な監視を怠っていたことが同法２２条に反すると指摘されている。

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シンフォーム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シンフォームに委託していたところ，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があることにつき予見可能性が認められ，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。

ウ　小括

したがって，被控訴人には，本件漏えい当時，シンフォームに対する適切な監督をすべき注意義務があり，これを怠った過失があったというべきである。

３　争点３（シンフォームは，Wによる本件漏えいについて使用者責任を負うか否か）について

民法７１５条１項の「ある事業のために他人を使用する者」とは，いわゆる

報償責任を認めたとする同法の趣旨に照らせば，広く使用者の指揮・監督の下に使用者の経営する事業に従事する者をいうと解される。

これを本件についてみるに，前記第３の１(3)のとおり，シンフォームは，被控訴人から委託を受けた業務について，外部の会社に再委託し，同社の従業員であったWが本件漏えいを行ったものであるところ，シンフォームとWの間には雇用関係はなく（争いがない），Wがシステムエンジニアとしてシンフォームに派遣され，シンフォーム多摩事務所で被控訴人の情報システムの開発等の業務に従事していたからといって直ちに，シンフォームとWの間に指揮監督関係があったとはいえない。

この点，控訴人は，シンフォームが，Wに対し，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するとともに，業務用パソコンを貸与し，業務開始時の入館証発行に当たっては研修を受けさせ，それ以降，毎年研修を実施していたから指揮監督関係があったと主張するが，これらの事実が認められたとしても，Wが実際に行っていた業務が，シンフォームと受託会社との間の業務委託契約に基づき受託会社の指揮監督の下に行われていたということと矛盾するものではなく，上記事実から直ちに，シンフォームがWの行う業務について具体的に指揮命令をしていたと認めることはできない。

この点につき，Wは，自身の刑事事件において，シンフォーム多摩事務所においては，シンフォームの社員から日常的に指示を受け，指揮監督を受けていた旨を述べている。しかしながら，一方で，Wは，再委託先の従業員に対し，自身が不在期間中の業務の代替人員の人選を依頼したことや，W自身のシンフォームにおける稼働時間の状況報告をしていた可能性があったことを認めており，また，シンフォームにおいて本件業務に関わっていたX及びYは，再委託先の要員に関しては，再委託先の管理者を通じて指揮監督を行っていた旨を供述しており，これらを裏付けるメールも残されていることからすると，シンフ

ォームが，Wに対して，その業務について具体的に指揮命令をしていたとまでの事実を認めることはできない。（甲７１，７２，７４，８１，乙１１６ないし１２６）

なお，シンフォームが，委託先に対し，個人情報保護法上の委託先の監督（同法２２条）を行うことがあったとしても，ここにいう監督は，委託先が，委託元との契約に沿って自ら業務を遂行したことに対し，委託元が，委託先の当該業務遂行について当該契約の条項に沿ったものであるか，法令を遵守しているか等をチェックするものであり，委託先の日常の業務を個別具体的に指示するものではなく，使用者責任における指揮監督とは異なるものであるから，この点は前記判断を左右するものではない。

そうすると，本件において，シンフォームとWの間に，使用者責任における指揮監督関係があったとはいえない。

したがって，使用者責任に関するその余の争点について判断するまでもなく，この点に関する控訴人の主張は理由がない。

４　争点４（被控訴人は，シンフォームの不法行為について使用者責任を負うか否か）について

被控訴人に使用者責任が認められるためには，前記３で説示したとおり，被控訴人とシンフォームの間に実質的な指揮監督関係があったと認められることが必要となる。

しかし，被控訴人とシンフォームとの間の契約は業務委託契約であり（争いがない），原則として，受託者が委託者の指揮監督を受ける内容のものではない。実際，前記第３の１⑶のとおり，シンフォームは，従前被控訴人において対応していた個人情報等の情報が増加したことに伴い，被控訴人からその管理業務の委託を受けたものであり，そのような経緯に照らせば，シンフォームにおいて，専門的知見に基づいて本件システムや本件データベースの運用管理を任されていたと認められ，被控訴人から具体的な指揮監督を受けていたとは認

められない。また，控訴人が指揮監督を基礎付ける事実として主張するものは，いずれも個人情報保護法上の委託先の監督を基礎付ける事実とはなり得るが，前記３で説示したとおり，同法上の委託先の監督と使用者責任における指揮監督とは異なるものであるから，これらの事実をもって直ちに使用者責任における実質的な指揮監督関係があったということにはならない。

したがって，この点に関する控訴人の主張は理由がない。

５　争点５（被控訴人らの共同不法行為責任）について

前記１及び２で説示したとおり，シンフォーム及び被控訴人は，それぞれ，固有の責任として，控訴人に対する不法行為責任を負うところ，当該被控訴人とシンフォームの不法行為は，被控訴人が保有し，その管理をシンフォームに委託していた本件個人情報の管理に関するものであり，客観的に関連することは明らかであるから，被控訴人らの不法行為は，共同不法行為（民法７１９条１項前段）に当たる。

６　争点６（控訴人らの権利侵害の有無）について

(1) 本件漏えいの対象となる控訴人らの個人情報

本件漏えいによって控訴人らの氏名，性別，生年月日，郵便番号，住所及び電話番号並びに控訴人及び選定者Ｂのメールアドレスが外部に漏えいしたことは当事者間に争いがない。なお，被控訴人は，受領した情報の真実性について個別に確認しているわけではないとしているが，控訴人らにおいて特に虚偽の情報を提供する理由はなく，真実のものであったというべきである。一方，これら以外の情報（選定者Ｃの続柄）については，これが漏えいしたことを認めるに足りる証拠はない。

(2) 控訴人らの権利侵害

漏えいした本件個人情報は，前記(1)のとおりであるところ，控訴人らが，これらの本件個人情報について，自己が欲しない他者にはみだりに開示されたくないと考えることは自然なことであるから，本件個人情報は，控訴人ら

のプライバシーに係る情報として法的保護の対象となるものであり，本件漏えいによって，控訴人選定者らは，そのプライバシーを侵害されたというべきである（最高裁平成２８年（受）第１８９２号平成２９年１０月２３日第二小法廷判決参照）。

この点，被控訴人は，被控訴人らの行為が社会通念上許容される限度を逸脱した違法な行為であるとみる余地はないと主張する。しかし，損害の有無及び程度の検討において被控訴人らの過失の内容やその経緯，事後の対応等を考慮する余地はあるとしても，被控訴人らの行為が社会通念上許容される限度を超えず違法性を欠くとはいえない。

7　争点７（控訴人らの損害の有無及びその額）について

(1) 本件個人情報は，被控訴人が集積した顧客情報の一部を構成するものであるが，氏名，郵便番号，住所，電話番号及びメールアドレスは，いずれも控訴人らの個人識別情報と連絡先であり，生年月日と性別も，日常的に契約等の際に開示することが多く，思想信条や性的指向等の情報に比べると，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」私的領域の情報という性質を強く帯びているとはいえない情報である。したがって，クレジットカード情報などの重要な情報と関連づけられて漏えいしていない本件のような場合，情報それ自体に重要な価値が認められるというより，顧客名簿として大量に集積されているところに価値が認められるのが通常であり，実際，本件においても，名簿業者に顧客名簿として売却され，被控訴人の同業者に渡りダイレクトメール等に利用されたことが認められる（なお，控訴人は，本件個人情報が，被控訴人という教育事業を行う企業の保有していた情報として漏えいしたことから，教育に熱心であるなど一定の評価が含まれる情報である旨主張するが，本件個人情報の流出元が被控訴人であることから，控訴人らの教育に関する何らかの思想や信条が推知されるとは考え難い。）。

(2) もっとも，本件個人情報は，これらを取得した者において，これらを取得

された者に対する連絡が可能となるものであるから，その使用方法いかんによっては，取得された者の私生活の平穏等に何らかの影響を及ぼすおそれがある。また，本件個人情報については，本件漏えいにより５００社を超える名簿業者に漏えいしたとの発表もあるところ，実際にどこまでの範囲に広がっているか確定は不能であり，回収も不可能といわざるを得ない。したがって，本件漏えいにより自己の個人情報を取得された者に対し，自己の了知しないところで個人情報が漏えいしたことに対する不快感及び生活の平穏等に対する不安感を生じさせることになるから，かかる不安感が具体的なものでなく抽象的なものであったとしても，何らかの精神的苦痛を生じさせることは避けられないことというべきである。

さらに，控訴人らが被控訴人に提供した本件個人情報について，自己の欲しない他者にみだりにこれが開示されることはないという控訴人らの期待は保護されるべきであり，控訴人らは，被控訴人において本件個人情報がみだりに流出することがないよう適切に管理されると信じて提供したのであるから，本件漏えいにより，このような期待が裏切られる結果となったことは明らかである。しかも，本件漏えいは，Wにおいて，高度な知識を応用したり，特殊な技術を駆使して行われたものではなく，単に，充電のため本件スマートフォンを市販のＵＳＢケーブルで業務用パソコンに接続したところ，データの転送が可能であったことから，思いつかれ実行されたものである。これまで述べてきたとおり，被控訴人らにおいて，自らが導入していた本件セキュリティソフトが適切に設定されているか否かを確認さえしていれば，煩雑な事務処理や多額の費用の支出を余儀なくされることもなく，比較的容易に本件漏えいを防ぐことができたのであるから，その意味においても，控訴人らの期待を裏切った度合いは小さくないというべきである。

したがって，前記６(2)のとおり，本件漏えいにより控訴人らはそのプライバシーを侵害されたものであるところ，上記認定に照らせば，控訴人らに

は，慰謝料の支払によって慰謝されるべき精神的損害が発生したと認めるのが相当である。

(3) 他方，控訴人らは，社会に拡散された本件個人情報が控訴人らの他の情報と関連付けられて重大なプライバシー情報が引き出される可能性を指摘するが，抽象的な可能性を指摘するものにすぎず，本件個人情報が個別に着目されて何らかの重大なプライバシー情報が引き出されることは想定しにくい。したがって，現時点においては，本件個人情報の漏えいは，控訴人らにおいて望まないダイレクトメールが増えるかもしれないという危惧を抱かせるにとどまるものであり，控訴人らに何らかの実害が発生したとは認められない。

また，被控訴人及びそ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，情報漏えいの被害の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った。そして，被控訴人は，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おり，控訴人らもそれぞれ電子マネーギフト５００円分を受領したことが認められるから，自己の個人情報が適切に取り扱われるであろうとの期待が侵害されたことについては，事後的に慰謝の措置が講じられていることが認められる。

(4) 以上のとおり，本件漏えいは，控訴人らに対し，不快感及び抽象的なものであるとはいえ不安感を生じさせるものであり，かつ，自己の個人情報が適切に管理されるであろうとの期待を裏切るものであるから，控訴人らには，慰謝料の支払によって慰謝すべき精神的損害が発生したといわざるを得ないところ，本件漏えいにより控訴人らに実害が発生したとは認められないこと，本件漏えいの発覚後，被控訴人及びベネッセホールディングスにおいて，直ちに被害の拡大防止措置が講じられていること，自己の個人情報が適切に扱われるであろうとの期待の侵害に対し，被控訴人において事後的に慰謝の措

置が講じられていること，その他本件にあらわれた一切の事情を総合すると，控訴人らの精神的損害に対する慰謝料の額は２０００円と認めるのが相当である。

なお，控訴人は，本件個人情報のうち，選定者Ｃの情報は，未成年者の情報であり，成年以上に保護の必要性が高いと主張するが，選定者Ｃの情報が未成年者の情報であるか否かは，慰謝料の額を左右するものとはいえない。

８　まとめ

以上のとおり，控訴人の請求は，被控訴人に対し，控訴人らそれぞれに２０００円及びこれらに対する遅延損害金の支払を命じる限度で理由があるから認容し，その余の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。

第６　結論

よって，控訴人の請求をいずれも棄却した原判決は相当でないから変更することとし，上記の限度で控訴人の請求を一部認容し，その余の請求をいずれも棄却することとして，主文のとおり判決する。

東京高等裁判所第１６民事部

裁判長裁判官　萩　原　秀　紀

裁判官　馬　場　純　夫

裁判官　杉　山　順　一