主　　文

1　一審原告らの控訴に基づき，原判決を次のとおり変更する。

⑴　一審被告らは，別紙控訴人目録の各「判断」欄に○と記載した一審原告らに対し，連帯して，それぞれ３３００円及びこれらに対する平成２６年７月７日から各支払済みまで年５分の割合による金員を支払え。

⑵　一審原告らのその余の請求をいずれも棄却する。

2　一審被告シンフォームの控訴を棄却する。

3　訴訟費用は，第１，２審を通じて，別紙控訴人目録の各「判断」欄に○と記載した一審原告らと一審被告らとの間においては，これを２０分し，その１９を同一審原告らの負担とし，その余を一審被告らの負担とし，同目録のその余の一審原告らと一審被告らとの間においては，全部同一審原告らの負担とする。

4　この判決は，第１項⑴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　一審原告ら

⑴　原判決を次のとおり変更する。

⑵　一審被告らは，別紙控訴人目録記載の一審原告らに対し，連帯して，それぞれ同目録の「請求額（円）」欄記載の金員及びこれに対する平成２６年７月７日から各支払済みまで年５分の割合による金員を支払え。

2　一審被告シンフォーム

⑴　原判決中，一審被告シンフォームの敗訴部分を取り消す。

⑵　上記敗訴部分にかかる一審原告らの一審被告シンフォームに対する請求をいずれも棄却する。

第２　事案の概要

1　本件は，一審原告らが，通信教育事業等を営む一審被告ベネッセに個人情報を提供していたところ，一審被告ベネッセからその管理を委託されていた一審被告シンフォームが更に外部業者に再委託をし，そこから更に業務委託を受けた先の会社の従業員において，私物スマートフォンを用いて当該個人情報を不正に取得し，それらを第三者に売却して外部に漏えいさせたことにつき，①一審被告らには一審原告らの個人情報の管理に係る注意義務違反があった，②一審被告シンフォームは前記従業員の使用者であり，前記従業員の行為につき使用者責任を負う，③一審被告ベネッセは一審被告シンフォームの使用者であり，一審被告シンフォームの注意義務違反につき使用者責任を負うなどと主張して，一審被告らに対し，プライバシーの侵害による共同不法行為又は使用者責任等に基づき，連帯して，一審原告らが被った精神的苦痛に対する慰謝料等の損害賠償金（上記漏えいの当時成年であった一審原告らにつき各５万円，未成年であった一審原告らにつき各１０万円）及びこれに対する不法行為の後の日である平成２６年７月７日から支払済みまで民法所定の年５分の割合による遅延損害金の支払を求める事案である。

2　原審は，①上記漏えいが，デジタルカメラの画像転送プロコトルをベースに，音楽・動画ファイルなどの転送を可能にした規格であるＭＴＰ（メディア・トランスファー・プロトコル〔Ｍｅｄｉａ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｃｏｌ〕の略）対応の私物スマートフォンを用いたものであり，一審被告らにおいて，上記漏えいの当時，そのような方法による情報漏えいに関する予見可能性はなかったとし，一審原告らの個人情報の管理に係る注意義務違反は認められないとした上で，②上記漏えいの当時，一審被告シンフォームと上記従業員との間には実質的指揮監督関係があり，一審被告シンフォームには上記漏えいについて使用者責任が成立すると認め，③一審被告ベネッセの使用者責任は否定して，一審被告シンフォームに対して，別紙控訴人目録の各「判断」欄に〇と記載した一審原告らに対し，それぞれ３３００円及びこれらに対する不法行為

の後の日である平成２６年７月７日から各支払済みまで民法所定の年５分の割合による遅延損害金の支払を求める限度で一審原告らの請求を認容した。

これに対して一審原告ら及び一審被告シンフォームが控訴をし，それぞれ前記第１の１及び２のとおりの判決を求めた。

なお，一審原告らは，当審において，一審被告らに対する請求元金の額を，上記漏えいの当時成年であった一審原告らにつき各２万円，未成年であった一審原告らにつき各４万円に減縮した。また，別紙控訴人目録の控訴人番号３６４の控訴人については，原審において遅延損害金の請求時期について平成２６年１２月９日（訴状送達の日の翌日）としていたが，当審において同年７月７日と改めた。

３　前提事実，争点及びこれに関する当事者の主張は，以下のとおり原判決を補正し，次項のとおり当審における一審原告らの補充主張を，次々項のとおり当審における一審被告らの補充主張を加えるほかは，原判決「事実及び理由」欄の「第２　事案の概要」の１項及び２項に記載のとおりであるから，これを引用する。ただし，「原告」を「一審原告」に，「被告ベネッセ」を「一審被告ベネッセ」，「被告シンフォーム」を「一審被告シンフォーム」にそれぞれ読み替える（以下同じ。）。

⑴　原判決３頁２５行目の末尾の次に，改行して「⑴　一審被告ベネッセ」を加え，同２６行目の「⑴」を削る。

⑵　原判決４頁１行目の末尾の次に，改行して「⑵　一審被告シンフォーム」を加え，同２行目の「⑵」を削る。

⑶　原判決４頁３行目の末尾の次に，以下のとおり加える。

「　一審被告らは，いずれも株式会社ベネッセホールディングス（以下「ベネッセホールディングス」という。）の子会社である。

⑶　一審被告ベネッセから一審被告シンフォームへの業務委託」

⑷　原判決４頁４行目の「⑶」を削り，同行目の「被告ベネッセは」の次に

「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，そのリスク管理のため，」を加える。

(5) 原判決４頁９行目の末尾の次に，以下のとおり加える。

「　一審被告シンフォームにおいては，本件システムに関する開発，運用及び保守の業務は，その顧客分析課が主な所管部署とされた。そして，一審被告シンフォームは，毎年，一審被告シンフォームの業務に従事する者（一審被告シンフォームの従業員であるかどうかにかかわらない。）の全員を対象として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) 一審原告らの一審被告ベネッセに対する個人情報の提供

一審原告らは，通信教育教材の取引，ベビー用品の通信販売の利用，情報サイトへの登録及びアンケートへの回答等をする際，一審被告ベネッセに対し，自ら及び未成年者の一審原告ら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。

(5) 本件システム及び本件データベースについて

ア　本件システムにおいては，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，一審被告ベネッセの事業部門は，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。

イ　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。

ウ　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。

一審被告らにおいて，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，一審被告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，また一審被告ベネッセにおいては，対応窓口となっていた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社のソフトウェアが，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）というソフトウェアが，それぞれ必要であった。（甲２，１９の３）

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

⑹　ａ（以下「ａ」という。）の本件業務への従事」

⑹　原判決４頁１０行目の「⑷」を削る。

⑺　原判決４頁１７行目の末尾の次に，以下のとおり加える。

「一審被告シンフォームは，本件システムの運用及び保守管理に関して外部業者に再委託をしており，ａは，そのような再委託先から更に順次委託を受けて一審被告シンフォームからみて３次委託先となる会社（以下「本件委託先会社」という。）の従業員であった。ａは，システムエンジニアとしての経験を有していた。

⑺　ａによる本件個人情報の漏えい」

⑻　原判決４頁１８行目の「⑸」を削り，同２１行目から２２行目にかけての括弧内を削る。

⑼　原判決４頁２４行目の「という。）。」の次に，「なお，本件当時，一審被告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，これらが，充電のために業務用のパソコンにＵＳＢケーブルで接続されていた。」を加える。

⑽　原判決５頁５行目の末尾の次に，改行して次のとおり加える。

「　本件漏えいの事実が発覚したことを受けて，警視庁生活経済課に対する取

材に基づき，ａが不正に取得した個人情報は，教育関連会社等の約５００社に流出したという報道がされた。（甲４９，５０）」

⑾　原判決５頁６行目の冒頭から２０行目の末尾までを次のとおり改める。

「⑻　本件漏えい当時に一審被告シンフォームが採用していた安全管理措置について

ア　インターネットとの接点

一審被告シンフォームは，データセンターに設置されているサーバと一審被告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，一審被告シンフォームは，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，重要なシステムに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。

イ　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。

ウ　内部ネットワーク

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。

エ　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，一審被告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，一審被告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一審被告シンフォームの各担当部門の部長に対して，メールでアラートが送信されるようになっていた。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，ａ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。（乙１及び弁論の全趣旨）

⑼　業務用パソコンに対するセキュリティ対策について

ア　一審被告シンフォームにおいては，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　一審被告らは，本件当時，情報漏えいを防止するため，業務用パソコンに株式会社日立ソリューションズ（旧商号・日立ソフトウェアエンジニアリング株式会社）の製品であるセキュリティソフトウェア「秘文Ｖｅｒ．９．０」（以下「本件セキュリティソフト」という。）を搭載させていた。本件セキュリティソフトは，本件当時，全てのデバイスについて，パソコンからデバイスへのデータの書き出し及びデバイスからパソコンへのデータの読込みを制御するという接続制御の機能を有していたが，一審被告シンフォームにおいては，本件セキュリティソフトにＭＴＰによる通信について接続を制御する設定を施していなかった。（甲１，１９の１ないし３，６９ないし７１，乙１）

⑽　データについて

一審被告シンフォームは，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（操作）ログの記録を全て取得して保管していた。（乙１及び弁論の全趣旨）

⑾　ＭＴＰとＭＳＣについて」

⑿　原判決５頁２１行目の「⑹」を削除する。

⒀　原判決６頁１１行目の末尾の次に，改行して次のとおり加える。

「⑿　本件漏えい後の一審被告らの対応について

ア　一審被告ベネッセは，平成２６年６月下旬，顧客から，一審被告ベネッセだけに登録した情報で他者から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。

一審被告ベネッセは，同年７月７日，一審被告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。

イ　一審被告ベネッセは，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。

ウ　一審被告ベネッセは，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，また，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。

一審被告ベネッセは，同月１４日以降，漏えいの確認された顧客らにお詫びの文書を送付し，その後，漏えいの確認された顧客らの選択に従って，当該顧客らに対してお詫びの品として５００円分の金券（電

子マネーギフト又は全国共通図書カード）を送付する方法又は漏えい１件当たり５００円を「財団法人ベネッセこども基金」（一審被告ベネッセ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。

エ　一審被告らの持株会社であるベネッセホールディングスのｂ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，一審被告ベネッセは，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。

（以上につき，甲１，１４の２及び３）

⑿　経済産業大臣の勧告について

経済産業大臣は，平成２６年９月２６日，一審被告ベネッセに対し，一審被告ベネッセは，①その保有する個人情報の利用・管理に責任を持つ部門を設定せず，その安全管理のため必要かつ適切な措置を講ずることを怠っており，個人情報の保護に関する法律（平成２７年法律第６５号による改正前のもの。以下「個人情報保護法」という。）２０条に違

反し，②顧客情報のシステム開発・運用に関する委託先である一審被告シンフォームに対して行う定期的な監査において，アラートシステムの対象範囲を監査の対象としていなかったなど，委託先に対する必要かつ適切な監督を怠っており，個人情報保護法２２条に違反するとして，個人情報保護法３４条１項に基づき，安全管理措置及び委託先に対する監督の徹底を勧告した。（甲１３の１及び２）

⑭　ａの刑事事件について

ａは，平成２６年７月１７日，警視庁によって不正競争防止法違反の被疑事実に基づき逮捕され，その後，本件漏えいに係る行為の一部について，一審被告ベネッセの営業秘密である顧客情報の不正領得及びその開示行為につき不正競争防止法違反の罪で起訴された。東京地方裁判所立川支部は，平成２８年３月２９日，ａについて不正競争防止法違反の犯罪の成立を認め，ａは顧客情報にアクセスする権限を与えられた者としての地位や専門的知識を悪用し，極めて大量の顧客情報を領得，開示した悪質な犯行を行ったものであり，その犯行の結果，一審被告ベネッセ及び関連会社の事業活動や経営状態に甚大な悪影響を与える事態となったなどとして，ａを懲役３年６月及び罰金３００万円に処するとの有罪判決を宣告した。ａはこれを不服として控訴し，控訴審である東京高等裁判所は，平成２９年３月２１日，ａの量刑不当の主張を容れ，ａが当該犯行に及んだ背景事情として，一審被告らにおける顧客情報の管理に不備があるとともに，被害が拡大したことに一審被告らの対応の不備があり，これらの被害者側の落ち度を考慮すべきであるのに第１審判決の量刑は重きに失するとして，第１審判決を破棄し，ａを懲役２年６月及び罰金３００万円に処するとの有罪判決（実刑）を宣告した。（甲３，１０，５２）

⑮　本件個人情報の漏えいの詳細」

⑭　原判決６頁１２行目の「(7)」を削る。

4　当審における一審原告らの補充主張

(1)　本件個人情報の漏えいにつき一審被告らには予見可能性があったことについて

以下のとおり，本件個人情報の漏えいにつき一審被告らの予見可能性を認めなかった原審の認定判断は不当である。

すなわち，一審被告らは，本件当時，スマートフォン等の外部機器による情報の不正取得を予見していたからこそ，そのような外部機器に対するセキュリティ対策を行っていたものである。そして，ＵＳＢメモリ等のＵＳＢ機器とパソコンとの間の通信方法として知られるＭＳＣ（マスストレージクラス〔Ｍａｓｓ　Ｓｔｏｒａｇｅ　Ｃｌａｓｓ〕の略）とＭＴＰによる通信方法とが異なる規格であることは事実であるが，一般的なセキュリティソフトウェアにおいては，このような通信方法に着目した設定がされるわけではなく，制御の対象となるデバイスの種別に応じて設定方法が提案されている。このことは，本件当時，一審被告らに使用されていた本件セキュリティソフト（秘文）においても同様であり，ＭＴＰによる通信方法に対応したスマートフォンを含め，ＭＴＰデバイスについては，ウィンドウズ・ポータブル・デバイス（以下「ＷＰＤ」という。）として書き出し制御の対象とする設定が可能であった。

本件当時，一審被告らの導入していた本件セキュリティソフトを含め，市販されていた多くのセキュリティソフトウェアがＷＰＤに対する制御機能を有しており，ＷＰＤが情報漏えいの危険性のある端末であることについては具体的に認識されていたといえる。実際に，一審被告シンフォームの担当者は，ａの刑事事件において，捜査機関に対しＷＰＤについても接続制御機能が有効になっていると考えていた旨述べていたのであり，一審被告らが，ＷＰＤによる情報持ち出しの危険性を認識していたことは明らかである。そして，一審被告らは，ＷＰＤを利用した情報漏えいが予見できたのであるから，

ＷＰＤの１機種であるＭＴＰ方式のスマートフォンによる情報漏えいについても予見可能性があった。

なお，一審被告らは，ＭＴＰによる通信方法に対応したスマートフォンによる情報漏えいについては結果回避義務がないなどと主張するが，本件セキュリティソフトにおいてＷＰＤについての接続制御機能を有効にする設定をしていなかったのは，クレジットカード情報等を含めた大量の個人情報を取り扱う業者としてリスク管理ができていなかったということにすぎず，結果回避義務がなかったなどということはできない。

⑵ 一審被告シンフォームの過失責任及び使用者責任が認められること

ア　過失責任について

一審被告シンフォームの過失の有無について，原判決が以下の注意義務違反を認めなかった点は不当である。

㋐ 原判決は，私物スマートフォンの持込み禁止について，執務室（オフィス）につき，持込みを禁止すべき注意義務がないなどとする合理的な理由を説明していない。執務室内には内線電話も設置されており，私物のスマートフォンは業務上使用する必要性がなかったのであるから，持込みを制限すべきであったことは明らかである。

㋑ また，本件では，アラートシステムが機能していれば情報漏えいを食い止めることができた。すなわち，ａは，平成２５年７月１７日から１８日に顧客情報２９万１５９１件を書き出してスマートフォンに保存し，同月１８日に株式会社セフティー（以下「セフティー」という。）にこれを売却している。その後は，同月２９日，同年８月６日に同様の方法で情報を持ち出し，以後も繰り返しているところ，ａがセフティーに売却した個人情報の合計件数１億７８９７万８９３３件（甲７６）に比較すると，最初の漏えい件数は全体のわずか１．６２パーセントであり，その段階でアラートシステムが機能していれば相

当割合の漏えいを食い止めることができた。また，アラートシステムが機能していることを掲示していれば，情報の持ち出しをすれば犯人が特定されることでａの犯行の動機を失わせることもできた。

イ　使用者責任について

使用者責任における指揮監督関係の有無は，実質的な観点から検討されるべきであるところ，ａは，その刑事事件における被告人質問（甲６３，６４）において，①作業ごとに所属していたグループにおいては一審被告シンフォームの従業員であるリーダーから作業を割り当てられ，打ち合わせへの出席指示を受け，作業スケジュールはリーダーが作成し，ＷＢＳと呼ばれる進捗管理表にやるべき作業・担当するメンバーを書き込んでいたこと，②ａが在籍するＡ社では，雇用契約上，Ａ社の従業員であるＴがａを指揮監督する者とされていたものの，ａの入社後１，２か月が経過した頃には，ＴとａはそれぞれＴ別のリーダーの下で作業をするようになり，Ｔも最初は毎日一審被告シンフォーム多摩事務所に来所していたが，そのうちに来所が週２日程度に減り，その後は全く来なくなったりしており，例外的に作業の問い合わせの電話連絡があった程度であったことを具体的に供述している。

また，一審被告シンフォームの事業開発本部長兼事業開発部長であったｃは，ａの刑事事件における証人尋問（甲７３）において，一審被告シンフォームの従業員とａのような他の委託先の従業員（以下「パートナー社員」ということがある。）が１対１でミーティングし，作業工程の確認をし合うことがあることや進捗状況の確認，計画通りに作業を終わらせるとの要望を出すことがあったこと，パートナー社員は一審被告シンフォームに直接作業報告をしていたことなどを認めており，具体的な指示や作業に関する監督があったといえる。

さらに，一審被告ベネッセと一審被告シンフォーム間の業務委託基本

契約書（甲３８）の６条においては，一審被告ベネッセの事前の書面による承諾のない業務の再委託が禁止されており，ａは，本件システム開発に関する事業について，実質的に一審被告シンフォームの従業員として勤務していたというべきである。

上記の点に関する原判決の認定判断は相当であり，一審被告らの主張には理由がない。

(3) 一審被告ベネッセの使用者責任が認められること

ア　一審被告シンフォームの使用者としての責任について

原判決は，一審被告らの関係が業務委託契約に基づくものであるという形式を重視して，一審被告ベネッセの使用者責任を否定したが，誤りである。

一審被告らグループ会社は，従来，一審被告ベネッセが現在行っている事業を行う親会社が存在し，一審被告シンフォームはその下でシステムを担当する機能的子会社であった。実質的にみれば，持株会社制に移行する以前は，一審被告シンフォームは，一審被告ベネッセのシステム部門がそのまま会社になった機能的子会社という位置付けにあり，一審被告ベネッセに従属する関係にあったから，実質的には一審被告ベネッセの指揮監督下にあったといえる。実際に，ａのようなパートナー社員も，一審被告ベネッセの担当者から直接指示を受けていた。ａは，一審被告ベネッセとの進捗会議に案件ごとに週１回参加していたし，一審被告ベネッセの管理職を担う者が，一審被告シンフォームの従業員を兼務して勤務していた。

イ　ａの使用者としての責任について（当審において追加された主張）

一審被告ベネッセは，自社のサーバーにあるシステムを開発するという業務において，ａに対して直接に指揮監督しており，ａの使用者にも該当する。このことは，一審被告らが互いに出向者を在籍させ，上記アで指摘したとおり，一審被告ベネッセの担当者が，ａを含むパートナー社員に対

して直接指示をして業務を行わせていたことなどから明らかである。

⑷　違法な権利侵害が認められること

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

⑸　一審原告らの損害が発生していること

個人情報の現代的価値や要保護性を軽視するのは相当でなく，一審原告らについては本件漏えいによる損害が認められるというべきであり，また，原判決が認定した損害額は不当に低額である。

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

一審被告ベネッセは，本件システムの開発や運用を，一審被告ベネッセとは契約上も関係性の希薄な者に担当させており，ＵＳＢケーブルで業務に必要のない私物スマートフォンをパソコンに接続することが常態化していることを長期にわたり黙認し，本件セキュリティソフトの設定を誤り，その見直しも行わず放置している間に本件漏えいが行われたものである。ａは，セフティーに対して１億７８９７万８９３３件の個人情報を売却したことが判明しており，他に２社の名簿業者にも個人情報を売却しているのであって，そこから更に情報が拡散した可能性は否定できず，捜査当局も拡散した先は５００社を超えるものと判断している。それらの情報の回収は困難であり，また，拡散した個人情報の悪用の危険性が高いことは明らかである。

５　当審における一審被告らの補充主張

⑴　本件漏えいに関する一審被告らの予見可能性について

本件漏えいに関して，一審被告らの予見可能性を肯定するためには，一審

被告らが従来の一般的なスマートフォンのパソコンへの接続方式（通信規格）はＭＳＣであって，本件セキュリティソフトの書き出し制御措置はＵＳＢによる接続方式（通信規格）がＭＳＣであれば機能するが，ＭＴＰであれば機能しないものであったこと，本件当時までに販売されるようになった一部のスマートフォンはＭＴＰによる通信方法に対応していたことを具体的に認識していたことが必要である。

しかるところ，一審被告シンフォームが本件セキュリティソフトを導入し書き出し制御措置を設定したのは平成２３年夏であったところ，その時点では，ＭＴＰに初めて標準対応したスマートフォン用ＯＳであるＡｎｄｒｏｉｄ４．０を搭載したスマートフォンも発売されていなかったのであって，一審被告シンフォームとしては，書き出し制御措置を講じることによってスマートフォン一般について書き出し制御できるものと考えていた。ＭＴＰによりＭＳＣデバイス制御に抜け道が生ずるという危険性については，本件当時，情報セキュリティの専門家においても認識されていなかったのであり，一審被告シンフォームは，本件セキュリティソフトの単なるユーザーにすぎず，セキュリティソフト会社から一部のスマートフォンには対応できない状態になっているなどの注意喚起を受けることもなかったのであって，そのようなセキュリティソフトウェアの穴に気付く契機はなかった。本件当時までにＭＴＰによる通信方法に対応したスマートフォンへの情報書き出しの危険性について具体的に指摘した行政機関その他の団体のガイドライン等はなかったのであり，一審被告らの予見可能性の有無については，例えば経済産業分野ガイドラインにおいて「しなければならない」とされている事項を充足していたかなどの観点から検討すべきである。ＭＴＰは，もともとデジタルカメラやデジタルビデオカメラ，携帯音楽プレーヤー，ボイスレコーダー等をウィンドウズパソコンに簡便に接続するために用いられていた技術仕様であり，本件当時，ＭＴＰによる通信を行う機器としては，スマートフォンは念頭に

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

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

⑵　一審被告シンフォームの過失責任及び使用者責任について

ア　本件セキュリティソフトは，そもそもＭＴＰにより通信をするデバイスに対する書き出し制御機能を有しておらず，ＭＴＰによる通信につき読み取りも書き出しも不可とする接続制御機能しか有していなかった。書き出し制御に関する注意義務違反につき，一審原告らの主張は，あらゆる機器へのパソコンへの接続を一律に禁止すべきであるかのようであるが，パソコンの使用によって得られる利便性を合理的根拠なく放棄すべきというに等しい暴論である。

イ　使用者責任について

原判決は，本件当時，一審被告シンフォームとａとの間に実質的指揮監督関係があったと判断したが，その判断の主な根拠となったのは，ａの刑事事件における供述内容のみである。

しかし，ａの刑事事件における供述内容は，一審被告シンフォームにおける仕事の割り振りや日常的な業務指示等の具体的場面について述べることなく，抽象的に，一審被告シンフォームの従業員であるリーダーが直接，委託先要員に仕事を割り振り，日常の業務指示をしていたという

結論のみを述べるものにすぎない。

ａは，刑事事件において，一審被告シンフォームから直接指揮命令を受けていたため，一審被告シンフォーム以下の契約関係は偽装請負であり公序良俗違反により無効であるから，ａが営業秘密を管理する任務を負っておらず無罪であるとの主張をしていたのであり，虚偽供述への強い動機があるとみなければならない。

⑶　一審被告ベネッセの過失責任及び使用者責任について

ア　一審被告ベネッセには，一審被告シンフォームに対してＭＴＰによる通信方法に対応したスマートフォンへの書き出し制御措置をとるよう指示すべき義務はなかった。委託業者と受託業者は，法人として異なるのであり，受託業者に業務遂行に当たり過失があったとしても，特段の事情がなければ委託業者に過失があることにはならない。一審被告ベネッセが，一審被告シンフォームに対し，適切に報告を求めていたとしても，一審被告ベネッセが書き出し制御措置の不十分な点に気付く可能性はなかったから，監督義務違反は認められない。

イ　システム開発やシステム保守運用その他委託元に常駐する形態の業務委託（かかる形態をとらざるを得ないのは，業務の性質上，必然的である。）について，問題が発生した場合にはすべからく委託元が指揮監督をしていたなどと判断するのは不当である。一審被告ベネッセと一審被告シンフォームとの関係は業務委託契約という対等な取引関係であり，一審被告ベネッセは，一審被告シンフォームの使用者とはいえないし，ａの使用者とされる具体的根拠は存在しない。

⑷　違法な権利侵害の有無について

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

性が弱く，また侵害行為の態様について社会的相当性の逸脱の程度が低いほど，違法性は否定されやすくなる。本件個人情報の内容や性質は，本来社会生活を送るうえでは当然明らかにされるべき個人識別などのための単純な情報にとどまり，情報の利用によって初めて個人の社会関係，取引関係，法律関係等の様々な関係が円滑に行われ得るものであって，秘匿されるべき性質のものとはいえず，被侵害利益の要保護性は低い。一審被告らの侵害行為の態様として悪質性がほぼ存在しないことや事後的に速やかな公表，補償，原因究明及び再発防止策の検討と実施を含む対応措置をとったことなどを考慮すれば，一般人の感受性を基準として，一審被告らの行為が，社会的に容認されないものとして違法であるとみる余地はない。

(5) 一審原告らの損害の発生の有無について

一審原告らが本件漏えいによる損害として主張するのは，抽象的な不安や不快感にすぎず，これによって平穏な生活を送る利益が害されるとは一般に考えられない軽微なものである。本件漏えいに係る行為の前後で一審原告らのおかれた具体的な立場や状況には変化がなく，損害は発生していない。秘匿性の高くない個人情報の流出に対して，具体的損害がないにもかかわらず損害の発生を認めて安易に損害賠償を認めることは，不法行為制度の目的からも正当化されるものではない。

本件漏えいによって，何らかの本件個人情報を取得した漏えい先が５００件を超えるという事実については客観的根拠がなく，一審原告らの個人情報が直接の売却先を超えて拡散した事実は何ら認められない。

第３　当裁判所の判断

当裁判所は，本件漏えいについて，一審被告らには一審原告らの個人情報の管理に係る注意義務違反があり，かつ，個人情報が漏えいした一審原告ら１人につき各３３００円の損害賠償請求（３０００円の慰謝料及び３００円の弁護士費用相当額）を認めるのが相当であると判断する。その理由は，以下のとお

りである。

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

⑴　ａの勤務状況と本件漏えい行為について

ア　ａは，システムエンジニアであり，本件システム構築等の業務について一審被告シンフォームから再委託を受けた会社から更に再々委託を受けた会社の従業員であった。ａは，平成２４年４月から，一審被告シンフォーム多摩事務所の執務室において稼働を開始し，顧客分析課の開発チームのグループに属して作業に従事していた。

一審被告シンフォームでは，事業開発本部の下に事業開発部がおかれ，事業開発部の中に顧客分析課が置かれており，顧客分析課が本件システム構築等の業務を所管していた。顧客分析課には，平成２６年６月当時，３９名が所属しており，そのうち一審被告シンフォームの従業員は１１名であり，その余の２８名は，ａを含む他の委託先の従業員であり，パートナー又はパートナー社員と呼ばれていた。

顧客分析課の中には複数のチームがあり，各チームの中には個別案件を効率的に進めるために少人数で構成された複数のグループがあり，各グループには，一審被告シンフォームの社員であるリーダーが置かれていた。そして，各グループでは少なくとも毎週１回は進捗会議が開かれ，同会議にはグループメンバー全員が参加して作業状況や作業予定等についての打合せがされていた。

（以上につき，甲１９の１ないし３，甲６３，６４，６６，７３，８８の１）

イ　ａは，一審被告シンフォームの業務に従事する前に，一審被告シンフォームから，業務上知り得た個人情報及び機密情報を開示・漏えいしないことを誓約する内容の「個人情報の取扱いに関する同意書」を提出し，

また，一審被告シンフォームが行う情報セキュリティ研修及びその内容を踏まえたテストを受け，その後も年１回実施される情報セキュリティ研修を受けていた。（前記前提事実⑶，甲２，１９の１ないし３，６３，８８の１）

ウ　ａは，平成２５年６月頃，経済的に困窮した状況であったことから，一審被告ベネッセの顧客情報を名簿業者に売却して金員を得ることを思いついたが，業務上用いていたパソコンには，ＵＳＢメモリ等の外部記録媒体を接続してもパソコンに認識されず，顧客情報を持ち出せない措置が講じられていたことから，そのようなことはできないと諦めていた。ところが，平成２５年７月頃，本件スマートフォンを充電するために市販のＵＳＢケーブルを用いて業務用パソコンのＵＳＢポートに接続し充電していたところ，パソコンにスマートフォンが外部記録媒体として認識され，パソコンの画面にスマートフォン内のフォルダが表示されたことから，試しにパソコンからファイルを転送してみたところ，スマートフォンに保存することができた。（甲６３，８８の１及び２）

エ　ａは，平成２５年７月頃から平成２６年６月頃までの間，一審被告シンフォーム多摩事務所において，一審被告ベネッセの顧客情報を業務用パソコンから本件スマートフォンに転送し，その内蔵メモリに保存する等の方法により個人情報を不正に取得した。

本件スマートフォンは，平成２４年秋冬期に発売された「ａｕ　ＨＴＣ社製　ＨＴＬ２１」という機種であり，ＯＳはＡｎｄｒｏｉｄ４．１であった。前記スマートフォンには，データ通信方法としてＭＴＰが初期設定されており，前記転送はＭＴＰを用いて行われたものであった。

（以上につき，前記前提事実⑺，甲１１の１及び２，甲１２の１及び２，６３，６４，８８の１及び２）

⑵　ＭＳＣとＭＴＰについて

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

ＭＳＣは，パソコンとＵＳＢメモリやメモリカード等のデバイスである外部記憶装置・媒体との間の情報通信方式として用いられているものであり，ＭＴＰは，Ｗｉｎｄｏｗｓ をＯＳとするパソコンと携帯機器との間で音楽・動画等のマルチメディア・データを簡便に共有・連携できるようにするためにマイクロソフト社が開発した規格であり，デジタルカメラの画像転送プロトコル（ＰＴＰ）をベースに，音楽・動画ファイルなどの転送を可能にした技術仕様である。

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

（以上につき，甲１５，１６，９８の１ないし４，乙３２，１１１）

イ　スマートフォンの主なＯＳには「ｉＯＳ」及び「Ａｎｄｒｏｉｄ」がある。ＭＴＰによる通信方法は，前記アの開発経緯から，従来は音楽・映像プレーヤーやデジタルカメラ等に利用されており，スマートフォンについては，「ｉＯＳ」はＭＴＰによる通信方法に対応していないが，「Ａｎｄｒｏｉｄ」については，平成２３年１０月１８日に発売されたＡｎｄｒｏｉｄ４．０以降のバージョンがＭＴＰによる通信方法に対応するようになった。

そして，株式会社ＮＴＴドコモ，ＫＤＤＩ株式会社及びソフトバンクグループ株式会社が平成２４年夏に発売したスマートフォンには，ＯＳを

Ａｎｄｒｏｉｄ４．０とするものが多数あり，また，電気通信事業者各社は，Ａｎｄｒｏｉｄ４．０より前のバージョンのスマートフォンについて，その頃以降，ＯＳのバージョンアップを提供した。なお，同年８月頃に発売されたサムスン製の「ＧＡＬＡＸＹ　ＳⅡ　ＷＩＭＡＸ　ＩＳ１１ＳＣ」の取扱説明書には，メディア転送モード（ＭＴＰ）でＵＳＢケーブルを用いてパソコンと当該スマートフォンを接続すると，パソコンに当該スマートフォンがポータブルデバイスとして認識され，当該スマートフォンとパソコンとの間でデータのやりとりができることが明記されている。

（以上につき，甲１６，５１の１ないし３，１０５の１ないし６，１１５，乙３２）

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

㈠　インターネット上の「モバイルトレンド」という連載において，平成２３年４月２７日に掲載された「スマートフォンのパソコン接続は大容量デバイスからＭＴＰへ（第１６４回）」と題する記事の中で，テクニカルライターの塩田紳二は，最近登場したＡｎｄｒｏｉｄスマートフォンやタブレットでは，パソコンとの接続にＭＴＰを使うものが増えてきたことを述べて，従来用いられてきたＭＳＣによる通信方法との違いについて説明をし，ＭＴＰを用いるメリットやデメリットに言及した上，今後はＭＳＣよりＭＴＰの方が便利な通信方法としてスマートフォンやタブレットでは，ＭＴＰを採用するものが増えていきそうであるなどと記載をした。（甲１５）

㈡　「日経ＰＣ２１」という雑誌において，平成２４年１２月２４日発売の２０１３年２月号版に掲載された「スマホはパソコンと連携して使

うのが正しい！　３つの方法を完全習得」と題する記事の中で，スマートフォンとパソコンとの間でファイルをやりとりする３つの方法のうち，１つがＵＳＢケーブルを用いて接続する方法としてＭＴＰ（メディア転送プロトコル）とＭＳＣ（大容量ストレージ）の２種類を指摘することができるところ，両方の方式が使えるスマートフォンならより簡単なＭＴＰを使うとよいこと，その方法によるとスマートフォンとパソコンをケーブル接続するだけでスマートフォン内の記憶装置がリムーバブルディスクとして表示されることなどが記載されていた。

前記記事は，平成２５年６月５日に「日経トレンディネット」のウェブサイト上にも掲載された。（甲１１６）

⑶　一審被告シンフォームによる安全管理措置及び本件セキュリティソフトの設定について

ア　一審被告シンフォームでは，業務での私物パソコンの使用を禁じ，全従業者個々人に対して，所定の設定がされた業務用パソコンを貸与した上，ＩＤを付与し，９０日に一度の頻度で変更を要するパスワードを設定させて利用させていた。業務用パソコンは，業務上の必要がない限り社外への持ち出しは禁止され，通常は施錠付きチェーンで各人のデスクに固定されていた。その他，本件当時，一審被告シンフォームが情報管理のために採用していた安全管理措置については，前記前提事実⑼記載のとおりである。（甲１９の１ないし３，乙２）

イ　一審被告シンフォームは，従業員に貸与していた業務用パソコンに本件セキュリティソフトを搭載しており，平成２３年７月に前記業務用パソコンのＯＳをＷｉｎｄｏｗｓ７にバージョンアップした際，本件セキュリティソフトも当時の最新版である「秘文Ｖｅｒ．９．０」にバージョンアップした。

本件セキュリティソフトは，前記のとおりバージョンアップされた際に，

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

（以上につき，甲６９ないし７１）

ウ　本件セキュリティソフトの販売代理店は，本件セキュリティソフトのバージョンアップの際，その設定作業を行ったところ，一審被告シンフォームとしては，特定のＵＳＢメモリ以外の全ての外部記録媒体への書き出しを制御するとの方針をとっていたが，実際には，本件セキュリティソフトのバージョンアップの際の設定内容は，「リムーバブル，ＣＤ／ＤＶＤ，外付けＨＤＤ」だけが書き出し制御の対象とされ，ＷＰＤを含む他のデバイスについては接続制御機能を有効とする設定が行われなかった。そして，前記販売代理店は，平成２３年８月，一審被告シンフォームに対してパラメーターシートを納品し，そこには，本件セキュリティソフトの設定内容として，「デバイス制御設定」欄の「①デバイス使用可否制御を有効にする，②デバイス個体識別制御を有効にする，③個体識別ログの出力を有効にする」の３つの項目のチェック欄にチェックがされておらず，設定されていないことが明示されていた。

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

（以上につき，甲１２の１及び２，６６，６９ないし７１）

エ　一審被告シンフォームは，本件漏えいが発覚した後の平成２６年７月２２日に本件セキュリティソフトのバージョンアップを行い，また，設定の見直しをして，「リムーバブル，ＣＤ／ＤＶＤ，外付けＨＤＤ」の書き出し制御機能の他に，イメージングデバイス，ＷＰＤ，ウィンドウズモバイル，ブラックベリー，無線ＬＡＮ，モデム，赤外線等のデバイスの接続制御機能を有効にした。（甲１９の１ないし３）

オ　商用デバイス制御ソフトの製品がＭＴＰ使用制限機能に対応した時期は，遅くとも以下のとおりであり，下記各製品の国内市場におけるシェアは，平成２６年６月時点で合計すると４３．５パーセントであったことが認められる。（甲１６，６９，９６の１ないし５，９７，１０１の１及び２，１０３の１，乙３５，１２３の１）

企業名	製品名	対応時期
日本電気株式会社	InfoCage	平成１９年７月
株式会社日立ソリューションズ	秘文 AE Information Fortress	平成２１年６月
エムオーテックス株式会社	LanScope Cat	平成２５年１０月
日本ファインアート株式会社	TotalSecurityFort	平成２３年８月

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

２　本件漏えいに関する一審被告らの予見可能性について

⑴　本件漏えいに係る行為は，ａにおいて，貸与されていた業務用パソコンから本件データベースにアクセスし，本件データベース内に保管されていた本件個人情報を抽出して業務用パソコンに保存した上，ＵＳＢケーブルを用いて，ＭＴＰによる通信方法に対応する本件スマートフォンに転送したというものである（前記前提事実⑺）。

このようなＭＴＰによる通信方法を用いたデータの転送については，もともとＭＴＰが，ＷｉｎｄｏｗｓをＯＳとするパソコンと携帯機器との間で音楽・動画等のマルチメディア・データを簡便に共有・連携できるようにするために開発された規格であり，パソコンとＵＳＢメモリやメモリカード等のデバイスである外部記憶装置・媒体との間の情報通信方式として，従来のスマートフォンで多く使用されていたＭＳＣとは異なる規格であったことに照らすと，一審被告らの本件漏えいに関する予見可能性の有無を検討するに当たっては，ＭＳＣに限らず，ＭＴＰによる通信方法を含め，これに対応したスマートフォンを用いた個人情報のデータの転送があり得ることについての認識可能性があったといえるかどうかを検討すべきものと解される。

⑵　そこで検討するに，本件当時も，スマートフォンをＵＳＢケーブルでパソコンと接続しデータのやりとりをすることが可能であることは一般的に知ら

れており，本件漏えいの以前から，例えば平成２１年経産省ガイドラインが，個人情報保護法の基本理念を踏まえ，個人情報保護の推進の観点からできるだけ取り組むことが望ましい事項の例として，「個人データを入力できる端末に付与する機能の，業務上の必要性に基づく限定（例えば，個人データを入力できる端末では，ＣＤ－Ｒ，ＵＳＢメモリ等の外部記録媒体を接続できないようにする。）」などと記載されており，外部記録媒体をパソコン等に接続する方法による情報漏えいのリスクが指摘されていたこと（甲７，９，乙１０）が認められる。

そして，前記認定事実のとおり，ＭＳＣとＭＴＰは，いずれもパソコンとこれに接続された各種デバイスとの間の情報通信方式（ファイル転送プロトコル）であって，本件漏えいに係るａの行為も，本件スマートフォンを充電するために市販のＵＳＢケーブルを用いて業務用パソコンのＵＳＢポートに接続し充電していたところ，上記パソコンにスマートフォンが外部記録媒体として認識されたため，試しに上記パソコンからファイルを転送してみたら，スマートフォンに保存することができたというものであって，格別専門的な知識や道具等を用いてデータの転送をしたわけではない。本件当時には，既にＭＴＰによる通信方法に対応したスマートフォンが多数発売され，又はＭＴＰによる通信方法に対応するようにバージョンアップすることも可能な状況であったこと（前記認定事実⑵），情報管理に関する社会一般の認識という観点からみても，株式会社日立ソリューションズを含めた相当数の大手業者が，本件漏えいが発覚する以前からＭＴＰ使用制限機能に対応した商用デバイス制御ソフトの製品を販売するようになっており（前記認定事実⑶），一審被告シンフォームも，平成２３年７月に本件セキュリティソフトをバージョンアップした際には，特定のＵＳＢメモリ以外の外部記録媒体についても書き出しを禁止するという方針をとっていたものであること（前記認定事実⑶），加えて，スマートフォンは，従来の通話機能のみを基本的な機能と

する携帯電話とは異なり，小型のパソコンともいえる多彩な機能を有する機器であって，年々バージョンアップによる機能の高度化が進むデバイスであることを併せ考慮すれば，一審被告らは，本件当時，ＭＳＣに限らず，ＭＴＰによる通信方法を含め，これに対応したスマートフォンを用いた個人情報のデータの転送があり得ることについても，想定することができた，すなわち，本件漏えいに関する一審被告らの予見可能性はあったというべきである。

(3) これに対し，一審被告らは，①実際には，本件漏えいの時点においてＭＴＰによる通信方法に対応したスマートフォンの国内シェアは小さかったし，商用デバイス制御ソフトの製品のうちＭＴＰ使用制限機能に対応したものもなかった，②本件漏えいによって初めて，スマートフォンを利用した個人情報の不正取得の危険性が認識されるようになったのであり，それ以前は専門家にとってもＭＴＰによる通信方法を利用したデータの転送により，ＭＳＣデバイス制御に抜け道が生ずるという危険性について一般的な認識とはなっていなかった，③本件当時までにＭＴＰによる通信方法に対応したスマートフォンへの情報書き出しの危険性について具体的に指摘した行政機関その他の団体のガイドライン等はなかったなどと主張する。

(4) 前記①について，一審被告らは，本件当時，ＭＴＰによる通信方法に対応したスマートフォンの国内シェアが少なかったことに関し，株式会社インターネットプライバシー研究所が作成した「携帯電話端末におけるＭＴＰ普及率についての調査報告」（乙３４）を提出し，そこには，スマートフォンと従来の携帯電話を併せた台数に対するスマートフォンの割合は，平成２４年３月末で２２％，平成２５年３月末で３６％，平成２６年３月末で４８％であり，ＭＴＰによる通信方法に対応したスマートフォン（「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による通信方法に対応したスマートフォンの出荷台数は，５９３万台余りということになる。

しかし，仮に前記の報告を前提にしたとしても，ＭＴＰによる通信方法に対応したスマートフォンの国内シェアについては，平成２３年１０月１８日に発売されたＡｎｄｒｉｄ４．０以降のバージョンがＭＴＰによる通信方法に対応するようになり，株式会社ＮＴＴドコモ，ＫＤＤＩ株式会社及びソフトバンクグループ等の大手業者が平成２４年夏に発売したスマートフォンには，ＯＳをＡｎｄｒｏｉｄ４．０とするものが多数出てきていたことや，ＯＳのバージョンアップも提供されていた事実（前記認定事実(2)）からすると，遅くとも本件当時までには，国内において，ＭＴＰによる通信に対応したスマートフォンの普及率が高まり，相当多数の台数が販売されるようになっていく状況にあったということができるのであるから，前記の報告が，ＭＴＰによる通信方法に対応したスマートフォンによるデータの転送について，一審被告らの予見可能性を否定するものとはいい難い。

また，前記①のうち商用デバイス制御ソフトの製品のうちＭＴＰ使用制限機能に対応したものもなかったという点について，一審被告らは，株式会社インターネットプライバシー研究所が作成した「端末管理・セキュリティ製品におけるＭＳＣ・ＭＴＰ制御機能についての調査報告」（乙３５）を提出し，そこには，平成２６年６月当時販売されていた主要な端末管理・セキュリティ製品について，実用的なＭＴＰ制御機能は，国内市場シェアが高い製品については全く搭載されておらず，実用的なＭＴＰ制御機能を搭載していたと認められる製品は，国内市場シェアが微少な１製品にとどまり，かつ初期設定ではＭＴＰ制御機能は無効とされていた旨の記載がある。しかし，前記報告においては，「実用的」の意味を「少なくとも読み取り専用の設定（リムーバルメディアからパソコンにデータを転送することは可能であるが，

パソコンからリムーバブルメディアにデータを転送することは不可能とする設定）ができる場合」と定義し，「実用的」でない製品についてはＭＴＰ制御機能を搭載していないものとして扱っているところ，情報セキュリティの観点からパソコンに保存されている情報を管理したり，当該パソコンを通じて情報を管理したりする場面において，リムーバブルメディアからパソコンにデータを転送すべき場合を想定する必要性に乏しく（甲１５によれば，もともとＭＴＰの規格は，音楽ファイル等を転送するために開発された規格であるとされている。），双方向の転送のいずれもが制限されることから情報セキュリティ上「実用的」でないとすることは不合理である。したがって，同報告は，その前提を欠くものといわざるを得ず，採用することはできない。

(5) また，前記②について，一審被告らは，特定非営利活動法人日本ネットワークセキュリティ協会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ｄの意見書（乙３２）を提出し，そこには，本件漏えいによって初めて，パソコンのリムーバブルメディアとしてスマートフォンを含む携帯電話が使用される危険性があることが認識され，セキュリティ業界がその対策をとるようになったのであり，大手セキュリティベンダーでさえ予見できていなかったものを，ユーザーである一審被告シンフォームが予見することは不可能であったという趣旨の記載がある。さらに，株式会社インターネットプライバシー研究所は，一審被告らから依頼を受けて複数の意見書等を作成し，平成２９年１月２３日付け意見書（乙２４）及び平成３０年９月２０日付け意見書（乙９６）の中では，本件当時，ＭＴＰによる通信方法に対応したスマートフォンによる情報漏えいのリスクは，情報セキュリティ専門家の間でもほとんど認識されていなかったと指摘し，平成３０年９月２０日付け意見書の中では，一般の企業等の業務において，デジタルカメラやボイスレコーダー等の画像・動画・音声の情報をＭＴＰによる通信方法によりパソコンに取り込むことは日常的に行わ

れており，ＭＴＰによる通信について読み取りを制御すれば，業務上大きな支障が生ずることを指摘している。そのほか，一審被告らは，本件漏えいの方法による情報漏えいの危険性を予見できなかったことについて情報セキュリティの専門家等の記事（乙３６，３７）や工学院大学名誉教授ｅが作成した平成３０年１月１５日付け意見書（乙９１）を提出しているところ，そこには，本件当時，ＭＴＰによる通信方法を利用した情報漏えいの危険性は知られていなかったとの認識についての記載がある。

しかし，本件当時までに，ＭＴＰによる通信方法に対応したスマートフォンを利用したデータの転送が可能であることについてメディア等に取り上げられたものがなかったわけではなく（前記認定事実⑵），前記のとおり，スマートフォンは小型のパソコンともいえる多彩な機能を有する機器であって年々バージョンアップによる機能の高度化が進むデバイスであり，実際にＭＴＰによる通信方法に対応したスマートフォンの普及率が高まるとともに，ＭＴＰ使用制限機能に対応した商用デバイス制御ソフトの製品が，平成１９年以降，平成２５年８月頃までには多数の販売業者によって販売されている状況下にあったこと，一審被告らも特定のＵＳＢメモリ以外の全ての外部記録媒体への書き出しを制御するとの方針の下で本件セキュリティソフトを搭載していたことからすれば，ＭＴＰによる通信方法に対応したスマートフォンへの情報書出しの危険性について具体的に指摘した行政機関等のガイドラインがなかったとしても，一審被告らにおいて，新たに登場したＭＴＰによる通信方法に対応したスマートフォンに対する情報漏えいの危険性があり，その対策の必要性があることについて認識し得たというべきである。

以上によれば，一審被告らが主張する前記②の点及び前記③の点について考慮したとしても，本件漏えいに関する一審被告らの予見可能性についての前記認定判断を覆すものとはいえない。

３　一審被告シンフォームの過失責任について

(1) 執務室への私物スマートフォンの持込み禁止について

本件において，ａが執務を行う部屋に，私物のスマートフォンを持ち込むことを禁止する措置をとっていれば，本件漏えいを回避できたということができるが，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込みを一切禁止するというのは，当該執務環境において従事する者にとって，非常に大きな制約となることは明らかであり，加えて，後記(3)に説示するとおり，同様の効果を上げられる他の代替手段があり得ることに照らすと，一審被告シンフォームにおいて，本件当時，執務室内に私物のスマートフォンの持込み禁止措置を講ずべき注意義務があったということはできない。

一審原告らは，①平成９年経産省基準には，「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平成２５年ＩＰＡガイドラインには，個人のノートパソコンやスマートデバイス等のモバイル機器及び携帯可能なＵＳＢメモリ等の外部記録媒体の業務利用及び持込みを制限しなければならない旨の指摘があり，③データセキュリティガイドブックには，共有区画として，オフィスとサーバー室に区別され，サーバー室については，脅威として情報の不正持ち出しの指摘とともに，管理策として記録媒体の持込み禁止ルールの記載があることに照らすと，一審被告シンフォームには，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　平成９年経産省基準について

確かに，平成９年経産省基準（甲６）には，「搬出入物」について，「情報システム等の運用に関連する各室の搬出入物は，必要な物に限定すること。」と記載されている。

しかし，当該記載から，私物スマートフォンを上記の搬出入物の対象

としているかどうか明らかとはいえない。かえって，平成９年経産省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，平成９年経産省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，平成９年経産省基準から，一審被告シンフォームについて当然に私物スマートフォンの執務室内への持込みを禁止すべき注意義務があるとは認められない。

イ　平成２５年ＩＰＡガイドラインについて

確かに，平成２５年ＩＰＡガイドライン（甲９）においては，個人のノートパソコンやスマートデバイス等のモバイル機器及び携帯可能なＵＳＢメモリ等の外部記録媒体の業務利用及び持込みを制限しなければならないとの指摘があるが，他方で，対策のポイントとして，持込み制限では，その場所で扱う重要情報の重要度及び情報システムの設置場所等を考慮する必要がある旨の記載があり，また，「重要情報の格納サーバやアクセス管理サーバ等が設置されているサーバルームでは，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，平成２５年ＩＰＡガイドラインは，いかなる業務が行われている部屋であっても同様の持込み制限を講じる必要があるという趣旨を示すものではなく，その扱う情報の重要度や情報システムの設置場所に応じた対策をとるべきとの趣旨を示すものであると解すべきである。そうすると，重要な情報が直接格納されているサーバの所在する場所では，外部記録媒体をより直接的にサーバ等の機器に接続することが可能であり，当該情報により直接的にアクセスすることが可能となることから，そのような可能性を高い確率で制限できる措置を執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，平成２５年ＩＰＡガイドラインは，必ずしもそのような厳しい制限をすることまで要求していないと解するのが相当である。

そうすると，平成２５年ＩＰＡガイドラインから，当然に私物のスマートフォンの執務室内への持込みを禁止すべき注意義務があるとは認められない。

ウ　平成２５年データセンターガイドブック

確かに，平成２５年データセンターガイドブック（甲２０）では，共有区画として，オフィスとサーバー室に区別され，サーバー室については，脅威として情報の不正持ち出しの指摘があり，管理策として記録媒体の持込み禁止ルールの記載があるが，他方で，オフィスについて，その脅威として不正侵入の指摘があるのみで，管理策として画像監視システムと入退管理システム（ＩＣカード・生体認証）の記載があるにとどまることに照らすと，平成２５年データセンターガイドブックの記載を根拠に，当然にスマートフォンの執務室内への持込み禁止措置をとるべき注意義務があるとは認められない。

したがって，この点に関する一審原告らの主張は理由がない。

⑵　業務用パソコンに対するＵＳＢ接続禁止措置について

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

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。一審原告らは，マウスについて，ＵＳＢポートによる接続以外の方法での接続が可能であると主張するが，どのようなマウスであっても別の方

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

したがって，一審被告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。

この点について，一審原告らは，①平成２１年経産省ガイドラインには，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平成２５年ＩＰＡガイドラインでは，個人の情報機器及び記録媒体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平成２２年ＪＩＳガイドラインでは，平成２１年経産省ガイドラインと同様の記載があることに照らすと，一審被告シンフォームには，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　平成２１年経産省ガイドラインについて

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

イ　平成２５年ＩＰＡガイドラインについて

確かに，平成２５年ＩＰＡ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，平成２５年ＩＰＡガイドラインの記載から，直ちにＵＳＢ接続の禁止措置を講ずべき注意義務があるとはいえない。

ウ　平成２２年ＪＩＳガイドラインについて

確かに，平成２２年ＪＩＳガイドライン（甲２２）では，平成２１年経産省ガイドラインでの前記アの指摘と同様の指摘がされているが，前記アで説示したとおり，そのことから直ちにＵＳＢポートを塞ぐ措置を講ずべき義務があるということはできない。

したがって，この点に関する一審原告らの主張は理由がない。

⑶　情報の書き出し制御措置について

ア　前記認定事実⑶のとおり，一審被告らが業務用パソコンに本件セキュリティソフトを搭載しており，その設定を変更して，ＷＰＤについて接続制御する設定にすれば，業務用パソコンからＷＰＤの一機種であるＭＴＰによる通信方法に対応したスマートフォンに対するデータの書き出しを防止することが可能であり，本件漏えいの方法による情報漏えいは防止できたことが明らかである。そして，一審被告シンフォームにおいて，本件当時，ＭＴＰ対応スマートフォンによる個人情報の漏えいの危険性について認識し得たところ，前記⑴及び⑵のとおり，スマートフォンの持込み禁止措置やＵＳＢ接続の禁止措置を講ずることは，業務従事者に対して過度の制約となり得ること等から一審被告シンフォームに前記各措置を講ずべき注意義務を認めることはできない中で，書き出し制御措置は実効性があり，かつ，業務従事者に対して必要以上に制約が生じない方法であるから，一審被告シンフォームにおいて，本件漏えい当時，ＭＴＰ対応スマートフォン

を含めて書き出し制御措置を講ずべき注意義務があったというべきである。

イ　これに対し，一審被告らは，①本件当時，スマートフォンに対する書き出し制御措置を執るべきと明示していたガイドライン等はなく，一審被告シンフォームの情報セキュリティ対策は十分に高度なものであったこと，②本件セキュリティソフトはＭＴＰにより通信をするデバイスに対しては読み取りも書き出しも不可とする接続制御機能しか有していなかったのであり，そのような接続制御をすることはパソコンの使用によって得られる利便性を合理的根拠なく放棄するに等しいなどと主張する。

しかし，前記①について，一審被告シンフォームは，本件個人情報を含む大量の個人情報を扱っていたところ，本件当時，ＭＴＰによる通信方法に対応したスマートフォンによる情報漏えいの危険性を予見することができ，これを回避するための書き出し制御措置をとることができたのであるから，ガイドライン等に記載がなかったことや同様の措置を執っている会社が少なかったとしても，前記認定判断が左右されるものではない。

また，前記②について，一審被告シンフォームは，本件漏えいが発覚した後，本件セキュリティソフトの設定を変更して，ＷＰＤにつき接続制御機能を有効にする設定に変更したことは，前記認定事実⑶ウ，エのとおりであって，これによって一審被告シンフォームの業務に特段の支障を来したという事情もうかがわれないことからすれば，一審被告シンフォームにおいて，ＷＰＤを業務用パソコンに接続させるデバイスとして用いる業務上の必要性があったとは認められず，本件当時，本件セキュリティソフトによりＷＰＤに対する接続制御措置をとることは可能であったということができる。

ウ　一審被告シンフォームは，平成２３年８月に本件セキュリティソフトのバージョンアップがされた際に，本件セキュリティソフトの取扱説明書

の記載や設定作業を行った販売代理店からの説明等によって，本件セキュリティソフトの設定内容次第であらゆるデバイスの接続制御措置をとることが可能であることを認識することができ，かつ，自らも作業手順を踏むことによって設定内容の変更も可能であったにもかかわらず，平成２６年７月に本件漏えいが発覚するまでの間，その設定内容の見直しがされた様子もなく，実際に設定内容の変更はされなかったものである（前記認定事実(3)ウ）。スマートフォンの高機能化が早い速度で進み，自らの情報セキュリティ対策の内容をそれに対応させるために一定程度の時間が必要であることを考慮しても，ＭＴＰによる通信方法に対応したスマートフォンであるＡｎｄｒｏｉｄ４．０が平成２３年１０月１８日に発売され，その後ＭＴＰによる通信方法に対応したスマートフォンの普及率が高まり，これに対応した商用デバイス制御ソフトの製品数も増加していった状況下において，遅くともａが本件個人情報を不正に取得するに至った本件当時（平成２５年７月頃から平成２６年６月頃）までには，本件セキュリティソフトの設定を見直し，適切な設定内容に変更する注意義務があったというべきであり，一審被告シンフォームにはこれに違反した過失があったといわざるを得ない。

(4) アラートシステムの設定義務違反について

一審被告シンフォームは，本件当時，連携システムについてはアラートシステムを設置していたことや，経済産業省の勧告（甲１３の２。以下「本件勧告」という。）でも本件データベースについてアラートシステムの対象となっていなかったことが指摘されていることからすると，アラートシステムの設置が情報セキュリティ対策として一定程度有効であった可能性は否定できない。

しかし，情報セキュリティ対策の中には，情報漏えい等の問題を事前に防ぐための対策から，何らかの問題が発生した場合に，その被害を最小限に食

い止めるための対策まで，種々のものがあるところ，一審原告らの主張するアラートシステムは，一定量の情報が一度に移動した際に，責任ある立場の者にアラート（警告）が送信され，当該状況に対してどのような対応をすべきかを判断する機会ができるというものであるから，情報漏えいを未然に防ぐことができるわけではない。また，どの程度の量の情報が移動した場合にアラートが発せられる設定とするかによって，それ以下の情報量であればアラートが発せられないことになり，必ずしも情報漏えいの全てを防ぐことができる対策ともいえない。特に，本件においては，一審被告シンフォームが，本件データベースが保存されているサーバと業務用パソコンとの間の通信量をアラートシステムの対象としていなかったのは，本件システムの開発が終了しておらず，本件システムに種々の不具合が生じており，サーバと業務用パソコンとの間で大量のデータ移動があったため，本件システムの運用開始前に前記通信量をアラートシステムの対象としてしまうことによって本件システムの開発に支障が生じかねないという理由があったこと（甲６５）からすると，前記通信量をアラートシステムの対象にするとしても，アラートが発生する基準値は相当高く設定せざるを得なかったと考えられるのであり，結局のところ，アラートシステムによって，有効に本件個人情報の流出を防止することが可能であったと断ずることはできないというほかない。

そうすると，本件において，一審原告らの主張するアラートシステムを設置したとしても本件漏えいを回避できたとは認められないから，この点に関する一審原告らの主張は理由がない。

(5) 監視カメラ等による監視義務違反について

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

しかし，証拠（乙２７）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，一審被告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ａが，本件漏えいの際に，監視カメラで確認することができ，かつ，通常の業務ではしないような行動をしていたのでない限り，現に設置されていたものより高精度な監視カメラの設置によっても本件漏えいを回避できたとは認められないところ，ａが，本件漏えいの際に，監視カメラで確認することができ，かつ，通常の業務ではしないような行動をしていたことを認めるに足りる証拠はない。

そうすると，本件において，本件漏えいの行われた執務室内に現に設置されていたものより高精度な監視カメラを設置していたとしても本件漏えいを回避できたとは認められないから，この点に関する一審原告らの主張は理由がない。

４　一審被告ベネッセの過失責任について

⑴　個人情報の利用・管理に責任を持つ部門設置に関する注意義務違反について

前記前提事実⒀及び証拠（甲３，７，１３の１及び２）によれば，経済産業分野ガイドラインにおいて，組織的安全管理措置の項目で，各項目を実践するために講じることが望まれる手法の例示として，「個人情報保護管理者（いわゆる，チーフ・プライバシー・オフィサー（ＣＰＯ））の設置」が挙げられているところ，①一審被告ベネッセは，本件漏えい以前，同社の法令遵守状況を管理監督する機関としてコンプライアンス部を設け，コンプライアンス部長をＣＰＯ（最高個人情報責任者）とし，その下に，専門部署とし

て個人情報保護課を設置し，個人情報保護活動を行っていたこと，②経済産業省は，一審被告ベネッセに対し，平成２６年９月２６日，同年１０月２４日までに個人情報保護法２０条に基づく安全管理措置及び同法２２条に基づく委託先の監督を徹底して，具体的な内容を報告するよう勧告し，勧告の原因として，本件漏えいの対象となったデータベースが，個人情報のダウンロードを監視する情報システムの対象として設定されていなかったところ，一審被告ベネッセは，一審被告シンフォームに対して行う定期的な監査において，当該情報システムの対象範囲を監査の対象としていなかった等，委託先に対する必要かつ適切な監視を怠っていたことが同法２２条に違反し，一審被告ベネッセの業務の全過程において同一審被告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，一審被告ベネッセにおいて，前記以上に適切な情報管理体制を構築するための組織が本件漏えいの前に存在していれば，情報セキュリティに関する情報を一元的に集約し，より組織的な対応ができた可能性は高まったといえるものの，より組織的な対応ができたからといって，かかる組織が本件漏えいまでにどのような具体的対応をすることができたのかは不明といわざるを得ず，本件漏えいを回避できたとは認められないから，この点に関する一審原告らの主張は理由がない。

⑵ 私物スマートフォンの持込み禁止，ＵＳＢ接続禁止措置，情報の書き出し制御措置，アラートシステムの設定及び監視カメラ等による監視に係る一審被告シンフォームと同様の注意義務について

一審原告らは，一審被告らは形式上別法人であるが，①一審被告ベネッセが，元々一審被告シンフォームの親会社であったものの株式会社ベネッセホールディングスを持株会社とするグループ企業に再編されたことや，②一審

被告シンフォームの役員に一審被告ベネッセの役員が就任していたことに照らすと，個人情報の管理・運用において，事業としての一体性が見られ，不法行為における責任主体としての一体性が認められると主張する。

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

したがって，一審被告シンフォームの過失は一審被告ベネッセの過失と同視できるから一審被告ベネッセの過失が認められるという一審原告らの主張は，その前提を欠き，理由がない。

⑶ 委託先選任及び監督に関する注意義務違反について

ア 委託先選任に関する注意義務違反について

一審被告ベネッセが，一審被告シンフォームを委託先として選任したことについて注意義務違反があったことを基礎付ける事実を認めるに足りる証拠はなく，この点に関する一審原告らの主張は理由がない。

イ 監督に関する注意義務違反について

個人情報保護法２２条は，「個人情報取扱事業者は，個人データの取扱いの全部又は一部を委託する場合は，その取扱いを委託された個人データの安全管理が図られるよう，委託を受けた者に対する必要かつ適切な監督を行わなければならない。」と規定し，平成２１年経産省ガイドライン（甲７）には，「必要かつ適切な監督」に関し，委託先を適切に選定すること，委託先に個人情報保護法２０条に基づく安全管理措置を遵守させるために必要な契約を締結すること，委託先における委託された個人データの取り扱い状況を把握することが含まれる旨の記載があり，ＪＩＳ基準（甲２２）は，「３．４．３．４ 委託先の監督」において，「事業者は，個人情報の取扱いの全部又は一部を委託する場合

は，十分な個人情報の保護水準を満たしている者を選定しなければならない。このため，事業者は，委託を受ける者を選定する基準を確立しなければならない。」，「事業者は，個人情報の取扱いの全部又は一部を委託する場合は，委託する個人情報の安全管理が図られるよう，委託を受けた者に対する必要，かつ，適切な監督を行わなければならない。」等と規定し，平成２２年ＪＩＳガイドライン（甲２２）は，「審査の着眼点」として，「委託先を選定する基準として，該当する業務については少なくとも自社と同等以上の個人情報保護の水準にあることを客観的に確認できること，選定基準は具体的で運用可能なものであること」等を例示していることに照らせば，大量の個人情報の運用管理を一審被告シンフォームに委託していた一審被告ベネッセには，本件漏えい当時，個人情報の管理について，委託先に対する適切な監督をすべき注意義務があったということができる。

そして，前記２で説示したとおり，一審被告ベネッセも一審被告シンフォームと同様に，本件当時，本件漏えいの方法による個人情報の漏えいの危険性を予見し得たものであって，一審被告ベネッセが，一審被告シンフォームに対し，本件セキュリティソフトのスマートフォンに対する書き出しないし接続制御機能への対応状況について適切に報告を求めていれば，ＭＴＰによる通信方法に対応したスマートフォンに対する接続制御機能に対応した設定・変更を指示することができたものであり，このような監督を行うことについて，一審被告ベネッセに過度の負担が生ずることもなかったと認められる。

そうすると，一審被告ベネッセには，本件当時，一審被告シンフォームにおける個人情報の管理につき，本件セキュリティソフトの設定・変更について適切に監督をすべき注意義務があったというべきであり，それにもかかわらず，一審被告ベネッセは，本件当時，業務用パソコンの

セキュリティソフトウェアの変更をすべき旨を指摘することなく放置していた（更新すらされていなかった）結果，本件漏えいを回避できなかったのであるから，前記注意義務に違反したといわざるを得ない。なお，本件勧告においても，一審被告ベネッセが，一審被告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個人情報保護法２２条に反すると指摘されていたところである。

以上のとおり，一審被告ベネッセには，本件当時，一審被告シンフォームに対する適切な監督をすべき注意義務があり，これを怠った過失があったというべきである。

５　違法な権利侵害の有無について

一審原告らにおいて，本件個人情報につき，自己が開示を欲しない第三者に対してはみだりに開示されたくないと考えることは自然なことであるから，本件個人情報は，一審原告らのプライバシーに係る情報として法的保護の対象となるものであり，本件漏えいの方法及び一審被告らの過失行為の内容等に照らし，本件漏えい行為によって，一審原告らは，違法にプライバシーを侵害されたというべきである（最高裁判所平成１５年９月１２日第二小法廷判決・民集５７巻８号９７３頁，最高裁判所平成２９年１０月２３日第二小法廷判決参照）。

一審被告らは，本件漏えいに係る行為が，社会通念上許容される限度を逸脱した違法な行為であるとはいえないと主張するが，一審被告らの過失行為の内容に加え，本件個人情報は，ａによって名簿業者に対して売却された上，当該業者から相当多数の企業に売却されたことがうかがわれ，もはやその回収は困難であることを考慮すると，本件漏えい行為に係る一審被告らの過失行為によって生じた本件漏えいが一審原告らの受忍限度の範囲内にとどまるとはいえない。損害の有無及び程度の検討において一審被告らの過失行為の

内容やその経緯，事後の対応等を考慮する余地はあるとしても，一審被告らの過失行為によって生じた本件漏えいが，社会通念上許容される限度を超えておらず，違法性を欠くとはいえない。

6　一審被告シンフォームの使用者責任について

⑴　ａについて，本件個人情報を不正に取得してこれを名簿業者に売却したことにつき，一審原告らのプライバシーを侵害する不法行為が成立することは明らかである。

⑵　民法７１５条１項の「ある事業のために他人を使用する者」とは，いわゆる報償責任を認めたとする同法の趣旨に照らせば，広く使用者の指揮・監督の下に使用者の経営する事業に従事する者をいうと解される。

そして，一審被告シンフォームは，一審被告ベネッセから委託を受けた業務について，外部の会社に再委託し，同社から更に再々委託を受けた会社の従業員であったａが本件漏えいを行ったものであるところ，一審被告シンフォームとａの間には雇用関係はなく（争いがない），ａがシステムエンジニアとして一審被告シンフォームに派遣され，一審被告シンフォーム多摩事務所で一審被告ベネッセの情報システムの開発等の業務に従事していたからといって直ちに，一審被告シンフォームとａの間に指揮監督関係があったとはいえない。

⑶　上記の点に関連して，ａは，自らの刑事事件において，一審被告シンフォームから直接指揮命令を受けていたため，一審被告シンフォーム以下の契約関係は偽装請負であり公序良俗違反により無効であるとの主張をするとともに，被告人質問（甲６３，６４）において，①所属していたグループでは一審被告シンフォームの社員であるリーダーから作業を割り当てられ，業務上の指示を受けていたこと，②ａが在籍するＡ社では，雇用契約上，Ａ社の従業員であるＴがａを指揮監督する者とされていたが，ａの入社後１，２か月が経過した頃にはＴとａは別のリーダー

の下で作業をするようになり，数か月後にはＴの一審被告シンフォーム多摩事務所への来所が週２，３日程度に減り，その後全く来なくなったりしていたなどの供述をしていたものである（甲１０，５２，６３，６４）。

しかし，上記供述内容を的確に裏付ける客観的証拠は見当たらず，かえって，一審被告シンフォームにおいて本件システムの開発等の業務に関わっていたｃ及びｆは，ａの刑事事件において，再委託先であるＡ社の従業員についてはＡ社の従業員である管理者を通じて人員や作業管理を含めた業務上の指揮監督を行っていたという趣旨の証言をしており，実際にそのような指揮監督が行われていたことをうかがわせるメールのやりとりを裏付ける書証（乙９８ないし１０８）も提出されている。ａの供述内容は，上記メールのやりとりについては記憶が曖昧であるとし，上記のとおり一審被告シンフォームのリーダーから直接業務上の指示を受けていた点を強調する一方で，Ａ社の従業員である管理者に対し，一審被告シンフォームにおける稼働時間の状況報告をしていたことや，自らが不在期間中の業務の代替人員の人選について依頼した可能性があることも供述していることなど一貫しない面があり，仮にＴが一審被告シンフォーム多摩事務所に来所する回数が徐々に減っていった事実があるとしても，システムエンジニアという職務の性質上，逐一相対して指示を受けながら作業をしなければならないとも考えにくいことなどを考慮すると，ａの上記供述内容のみから，一審被告シンフォームとａとの間で実質的な指揮監督関係があった事実を認めることは困難であるといわざるを得ない。

(4) 一審原告らは，一審被告シンフォームが，ａに対し，一審被告シンフォームの顧客分析課長等の許可を受けた従業員を通じて業務用アカウントを教示するとともに，業務用パソコンを貸与し，業務開始時の入館証発

行に当たっては研修を受けさせ，それ以降，毎年研修を実施していたから指揮監督関係があったとも主張するが，これらの事実が認められたとしても，ａが実際に行っていた業務が，一審被告シンフォームと受託会社（Ａ社）との間の業務委託契約に基づき受託会社の指揮監督の下に行われていたということと矛盾するものではなく，前記事実から直ちに，一審被告シンフォームがａの行う業務について具体的に指揮命令をしていたと認めることはできない。

なお，一審被告シンフォームが，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。また，一審被告ベネッセと一審被告シンフォーム間の業務委託契約において業務の再委託が原則として禁止されていたとしても，上記認定判断を左右するものではない。

したがって，一審被告シンフォームの使用者責任に関するその余の争点について判断するまでもなく，この点に関する一審原告らの主張は理由がない。

7　一審被告ベネッセの使用者責任について

(1)　一審被告シンフォームの使用者としての責任について

一審被告ベネッセと一審被告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。一審被告シンフォームは，従前一審被告ベネッセにおいて対応していた個人情報等の情報が増加したことに伴い，一審被告ベネッセからその管理業務の委託を受けたという経緯に照らせば，

一審被告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，一審被告ベネッセから具体的な指揮監督を受けていたとは認められない。また，一審原告らが指揮監督を基礎付ける事実として主張するものは，いずれも個人情報保護法上の委託先の監督を基礎付ける事実とはなり得るが，前記６で説示したとおり，同法上の委託先の監督と使用者責任における指揮監督とは異なるものであるから，これらの事実をもって直ちに使用者責任における実質的な指揮監督関係があったということにはならない。

一審原告らは，持株会社制に移行する以前は，一審被告シンフォームは，一審被告ベネッセのシステム部門がそのまま会社になった機能的子会社という位置付けにあり，一審被告ベネッセに従属する関係にあったなどと主張するけれども，そのような事情を考慮したとしても，上記認定判断を左右するものではない。

したがって，この点に関する一審原告らの主張は理由がない。

⑵　ａの使用者としての責任について

一審被告ベネッセとａの間には雇用関係はなく（争いがない），ａがシステムエンジニアとして一審被告シンフォームに派遣され，多摩事務所で一審被告ベネッセの情報システムの開発等の業務に従事していたからといって直ちに，一審被告ベネッセとａの間に指揮監督関係があったとはいえない。そして，上記⑴のとおり，一審被告ベネッセが一審被告シンフォームに対して実質的な指揮監督をしていたとはいい難く，また，一審被告シンフォームがａに対して実質的な指揮監督をしていたともいえないのであって，それらの関係とは別に，一審被告ベネッセにおいて，一審被告シンフォームとの間の業務委託契約に基づく業務の範囲を超えて，直接，ａに対して，本件システムの開発に関わる日常業務につき具体的な指示をするなど，実質的な指揮監督関係を及ぼしていたことを裏

付ける的確な証拠はなく，一審原告らの上記主張を認めるには足りない。

8　一審被告らの共同不法行為責任について

前記２ないし５で説示したとおり，一審被告シンフォーム及び一審被告ベネッセは，それぞれ，固有の責任として，一審原告らに対する不法行為責任を負うところ，当該一審被告らの不法行為は，一審被告ベネッセが保有し，その管理を一審被告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，一審被告らの不法行為は，共同不法行為（民法７１９条１項前段）に当たるということができる。

9　一審原告らの個人情報の漏えいの有無及び範囲について

本件漏えいに係るａの行為によって一審原告らの個人情報が漏えいしたか否か及び漏えいした場合の情報の範囲については，原判決の「第３　争点に対する判断」の１項に記載のとおりであるから，これを引用する。

10　本件漏えいによる一審原告らの損害の発生の有無及びその額について

⑴　本件漏えいによって，一審原告らの氏名，性別，生年月日，郵便番号，住所，電話番号，ファクシミリ番号，メールアドレス，出産予定日及び保護者の氏名といった情報が漏えいしたものであるところ，このうち，氏名及び郵便番号・住所，電話番号，ファクシミリ番号及びメールアドレスについては，これらの情報を取得した者において，これらを取得された者に対する連絡が可能となり，また，同情報の使用方法によっては，取得された者の私生活の平穏等に一定の影響が及ぶおそれがある。また，一審原告らがこれらの情報を提供した経緯及び情報の内容に照らし，これらの情報がみだりに第三者への開示がされることはないとの期待が存在したものと考えられ，性別，生年月日，出産予定日及び保護者の氏名も含め，自己の了知しないところで第三者に流出することは欲しないものであったということができるから，これらの情報が不正に漏えいした場合には，自己の了知しないところで自己の個人情報が漏えいしたことへの私生活上の不安，不快感及び失望感を生じさせた

ものとして，精神的損害が生じたと認めるのが相当である。

⑵ もっとも，出産予定日を除くこれらの情報は，人が社会生活を営む上で一定の範囲の他者に開示することが予定されている個人を識別するための情報又は個人に連絡をするために必要な情報でもあるため，思想・信条，病歴，信用情報等とは異なり，個人の内面等に関わるような秘匿されるべき必要性が高い情報とはいえない。また，出産予定日については，予定日にすぎないので，秘匿されるべき必要性の程度が相対的に低い。さらに，一審原告らは，本件漏えいでは，一審原告らについて，子供の教育に熱心な，若しくは関心がある親又は教育に熱心な，若しくは関心がある親に育てられた子という属性も流出していると主張するけれども，ａはイベントで集めた情報などとして本件個人情報を売却しており，情報の量や質から一審被告らが保有していた情報として漏えいしたことが推測されていたとしても，これらの属性も，秘匿性が高いものとはいえず，それによって，一審原告らの精神的損害の程度が高まるものということはできない。

また，本件漏えいに係る情報は，一審原告らそれぞれでその範囲を異にし，その内容も異なるところ，自己の提供した個人を識別するための情報や個人に連絡するために必要な情報を漏えいされたこと自体には違いはなく，その範囲や内容によって，自己の了知しないところで自己の個人情報が漏えいしたことへの不安，不快感等につき，精神的損害の程度を区別して考えるほどの違いがあるとまではいえない。

なお，一審原告らは，未成年の一審原告らに関しては，不安，不快感がこれから一生付きまとうなどして，精神的苦痛は成年者とは異なるとも主張するが，本件漏えいによる影響の期間は，成年者であるか未成年者であるかを問わず，個別の事情によるところが大きい一方，自己の了知しないところで自己の個人情報が漏えいしたことへの不安，不快感の程度は，成年者であるか未成年者であるかは問わず，異なるものとはいえないため，成年原告と未

成年原告とで精神的損害の程度を格別に扱う理由までを見いだすのは困難であるので，同主張は採用しない。

(3) そして，本件漏えいにより，教育関連会社等５００社を超える会社に情報が流出したとの報道がされている上，本件漏えいの発覚経緯が，一審被告ベネッセの顧客から，一審被告ベネッセに対し，一審被告ベネッセと異なる通信教育事業者から一審被告ベネッセに提供していた氏名を名宛人とした書面が送付されているとの指摘が多数寄せられ，しかも，その氏名の中には，一審被告ベネッセだけに提供していた戸籍上の氏名と異なるものがあるとの指摘が含まれていることに鑑みると，本件漏えいに係る情報も同通信教育事業者に流出した可能性があるといえるものの，一審原告らもダイレクトメールやセールス電話が一審原告ら全員に生じているとまでは主張しておらず，前記の流出の可能性を超えて，現時点で，ダイレクトメール等が増えたような気がするという程度以上に財産的損害その他の実害が一審原告らに生じたことはうかがわれない。

一方，一審被告シンフォームは，ａから，個人情報等を漏えいしない旨記載された同意書を取得していたほか，ａに対して，情報セキュリティ研修等を受講させていた。そして，一審被告ベネッセの持ち株会社である株式会社ベネッセホールディングスは，本件漏えいの発覚後に直ちに対応を開始し，情報漏えいの被害拡大を防止する手段を講じ，監督官庁に対する報告及び指示に基づく調査報告を行い，情報が漏えいしたと思われる顧客に対し，本件通知書を送付するとともに，顧客の選択に応じて５００円相当の謝罪品の交付を申し出るなどしている。

以上のとおり，本件に現れた一切の事情を総合考慮すると，個人情報の漏えいした一審原告らにつき本件漏えいに係る不法行為によって生じた精神的損害に対する慰謝料として３０００円を認めるのが相当である。

そして，一審原告らが一審原告ら訴訟代理人弁護士に本件訴訟の提起及び

追行を委任したことは当裁判所に顕著であるところ，その弁護士費用としては，本件事案の難易，請求額，損害額その他諸般の事情を考慮すると，一審原告１人当たり３００円の範囲内のものが一審被告らの不法行為と相当因果関係にある損害とみるのが相当である。

11　小括

以上によれば，一審被告らは，共同不法行為（民法７１９条１項前段）に基づき，連帯して，別紙控訴人目録の「判断」欄に〇と記載した一審原告らに対し，同一審原告らそれぞれにつき３３００円及びこれに対する不法行為の後の日である平成２６年７月７日から支払済みまで民法所定の年５分の割合による遅延損害金の限度で支払義務を負う。

第４　結論

以上によれば，原判決中，一審原告らの一審被告ベネッセに対する請求を全部棄却した点は相当でないからこれを変更し，上記の限度で一審原告らの請求を一部認容し，その余の請求をいずれも棄却することとし，一審被告シンフォームの控訴は棄却することとして，主文のとおり判決する。

東京高等裁判所第２３民事部

裁判長裁判官　　白　　石　　哲

裁判官　　筒　　井　　健　　夫

裁判官　　加　　本　　牧　　子