令和５年２月２７日判決言渡　同日原本領収　裁判所書記官

平成２７年（ワ）第２２３６号　損害賠償請求事件（以下「第１事件」という。）

平成２７年（ワ）第５３７７号　損害賠償請求事件（以下「第２事件」という。）

平成２７年（ワ）第１４５６９号　損害賠償請求事件（以下「第３事件」という。）

平成２７年（ワ）第２８０７９号　損害賠償請求事件（以下「第４事件」という。）

平成２９年（ワ）第１７５０３号　損害賠償請求事件（以下「第５事件」という。）

口頭弁論終結日　令和４年１０月２４日

判　　決

主　　文

１　被告ベネッセＣｏ及び被告シンフォームは、別紙６－１第１事件認容原告番号目録記載の各原告に対し、連帯して、それぞれ３３００円及びこれに対する平成２７年４月３日から支払済みまで年５分の割合による金員を支払え。

２　被告ベネッセＣｏ及び被告シンフォームは、別紙６－２第２事件認容原告番号目録記載の各原告に対し、連帯して、それぞれ３３００円及びこれに対する平成２８年２月２７日から支払済みまで年５分の割合による金員を支払え。

３　被告ベネッセＣｏ及び被告シンフォームは、別紙６－３第３事件認容原告番号目録記載の各原告に対し、連帯して、それぞれ３３００円及びこれに対する平成２８年１０月４日から支払済みまで年５分の割合による金員を支払え。

４　被告ベネッセＣｏ及び被告シンフォームは、別紙６－４第４事件認容原告番号目録記載の各原告に対し、連帯して、それぞれ３３００円及びこれに対する平成２９年１１月７日から支払済みまで年５分の割合による金員を支払え。

５　被告ベネッセＣｏ及び被告シンフォームは、別紙６－５第５事件認容原告番号目録記載の各原告に対し、連帯して、それぞれ３３００円及びこれに対する平成２９年１１月３日から支払済みまで年５分の割合による金員を支払え。

６　原告らのその余の請求をいずれも棄却する。

７　訴訟費用は、全事件を通じて、これを２０分し、その１を被告ベネッセＣｏ

及び被告シンフォームの負担とし、その余を原告らの負担とする。

８　この判決は、第１項から第５項までに限り、仮に執行することができる。

事 実 及 び 理 由

第１　請求

１　第１事件

被告らは、第１事件原告らに対し、連帯して、それぞれ５万５０００円及びこれに対する平成２７年４月３日から支払済みまで年５分の割合による金員を支払え。

２　第２事件

被告らは、第２事件原告らに対し、連帯して、それぞれ５万５０００円及びこれに対する平成２８年２月２７日から支払済みまで年５分の割合による金員を支払え。

３　第３事件

被告らは、第３事件原告らに対し、連帯して、それぞれ５万５０００円及びこれに対する平成２８年１０月４日から支払済みまで年５分の割合による金員を支払え。

４　第４事件

被告らは、第４事件原告らに対し、連帯して、それぞれ５万５０００円及びこれに対する平成２９年１１月７日から支払済みまで年５分の割合による金員を支払え。

５　第５事件

被告らは、第５事件原告らに対し、連帯して、それぞれ５万５０００円及びこれに対する平成２９年１１月３日から支払済みまで年５分の割合による金員を支払え。

第２　事案の概要等

１　事案の概要

原告らは、主としてこども向けの通信教育事業等を営む被告ベネッセＣｏに対して氏名、住所等の個人情報を提供していたところ、被告ベネッセＣｏから委託を受けてその保有する顧客等についての情報の使用に関するシステムの開発、保守及び運用の業務に従事していた被告シンフォームのいわゆる３次委託先の業者の従業員が、その所有するスマートフォンを用いて原告らを含む上記の顧客等についての個人情報を取得した上で第三者に売却して外部に漏えいさせたことにより、原告らのプライバシーが侵害され、精神的苦痛を被ったと主張している。

本件は、原告らが、①被告シンフォームに対しては、情報の漏えいを防止する措置を講じなかったことを理由とする不法行為責任又は上記従業員を被用者とする使用者責任を、②被告ベネッセＣｏに対しては、委託先の選定及び監督を怠ったことを理由とする不法行為責任又は被告シンフォームを被用者とする使用者責任を、③被告ベネッセＨＤに対しては、ベネッセグループを統括し、被告ベネッセＣｏ及び被告シンフォームの全株式を保有する立場として、グループ全体における個人情報の利用・管理に責任を持つ部門を設置しなかったこと等を理由とする不法行為責任をそれぞれ負うとするとともに、被告らには共同不法行為が成立するとして、被告らに対し、原告１人当たり５万５０００円（慰謝料５万円及び弁護士費用５０００円）の損害賠償金及びこれに対する不法行為以後の日（各事件の訴状送達の日の翌日）から各支払済みまで平成２９年法律第４４号による改正前民法所定の年５分の割合による遅延損害金の連帯支払を求める事案である。

２　前提事実

以下の事実は、当事者間に争いがないか、後掲各証拠（特記なき限り枝番は省略）及び弁論の全趣旨により容易に認められる。

⑴　当事者等

ア　被告ベネッセＨＤ（旧ベネッセコーポレーション）は、通信教育、模擬

試験の実施や雑誌等の発行・通販事業などを目的として昭和２２年１１月２１日に設立された株式会社である。同社は、ベネッセグループを統括する会社であり、被告ベネッセＣｏ及び被告シンフォームの株式全部を保有する完全親会社である。

被告ベネッセＨＤの平成２６年６月２１日時点の発行済株式総数は１億０２４５万３４５３株であり、同年３月期決算（平成２５年４月１日～平成２６年３月３１日）における連結売上高は４６６３億９９００万円、連結純利益は１９９億３０００万円、単体純利益は１０６億１７００万円、連結総資産は４８７５億９４００万円、単体純資産は２０５２億０７００万円である。

イ　被告ベネッセＣｏは、通信教育、模擬試験の実施や雑誌等の発行・通販事業などを目的として平成２１年１０月に設立された株式会社である。

ウ　被告シンフォームは、コンピュータ等のシステム・ソフトウェアの開発や導入指導や情報処理サービスなどを目的として昭和４６年７月２７日に設立された株式会社である。

被告シンフォームは、被告ベネッセＣｏから委託を受けて、システムの開発・運用を行っている。

（争いがない。弁論の全趣旨）

⑵　被告らの関係及び被告ベネッセＣｏの顧客情報へのアクセス方法

ア　被告ベネッセＣｏは、従前から、主に、顧客管理システム及び販売管理システムに大別される複数のデータベースに顧客等（被告ベネッセＣｏの顧客のほか、被告ベネッセＣｏが契約によらずに本人の同意を得て個人情報を取得した者を含む。）の個人情報（以下「顧客情報」と総称する。）を集積して事業活動に利用していたが、リスク管理と効率化を図るため、平成２４年４月頃、被告シンフォームに対し、複数のデータベースに分かれて集積されていた顧客情報を統合し、統合したデータベース（以下「本

件データベース」という。）から必要な情報を抽出して分析に使用するためのシステム（以下「本件システム」という。）の開発・運用・保守の各業務（以下「本件業務」という。）を委託した。

被告シンフォームは、本件業務の一部を、更に複数の業者に対して委託した。

（甲５、１７、４２、５３、６５、６７、８７、８８、弁論の全趣旨）

イ　被告ベネッセＣｏのサーバコンピュータに保存されている本件データベース内の顧客情報にアクセスする方法としては、①被告シンフォームがその業務従事者に貸与するパーソナルコンピューター（以下「パソコン」といい、一般に企業が業務従事者に貸与するパソコンを「業務用パソコン」という。）から直接アクセスする方法と、②バッチ処理（一定量のデータを集め、一括処理をする方法）を行うバッチサーバを経由してアクセスする方法の二つがあったが、上記①の方法でアクセスする場合にはオラクル社のソフトウェアが、上記②の方法でアクセスする場合にはテラタームというソフトウェア（インターネット接続ができれば誰でも無料でダウンロード・インストールが可能なフリーソフトウェア）が必要であった。そして、上記いずれの方法による場合も、本件データベースにアクセスするためには、ＩＤ及びパスワードが必要であったほか、上記②の方法でアクセスする場合には、さらに、バッチサーバにアクセスするための別個のアカウントも必要であった。

（甲５、１７、５３、６５～６８、８７、８８、弁論の全趣旨）

⑶　Ａの業務状況

ア　Ａ（以下「Ａ」という。）は、本件業務に関しては、被告シンフォームからみて３次委託先（被告ベネッセＣｏからみると４次委託先）となる法人の従業員であり、システムエンジニアとして本件業務に従事していた。

Ａは、平成２４年４月頃から、被告シンフォームの東京支社多摩事務所

（以下「多摩事務所」という。）において、本件データベースにアクセスするためのＩＤ及びパスワード等を付与され、被告シンフォームから貸与を受けた業務用パソコン（以下「本件パソコン」という。本件パソコンには、前記⑵イのオラクル社のソフトウェア及びテラタームが搭載されていた。）を使用して、本件業務に従事するようになった。

（甲５、１７、５３、６５、６６、７５、８７、８８、弁論の全趣旨）

イ　被告シンフォームの業務用パソコンのオペレーティングシステム（以下「ＯＳ」という。）は、平成２３年７月以降、Ｗｉｎｄｏｗｓ７であった。

Ｗｉｎｄｏｗｓ７は、パソコンとこれに接続されたデバイス（周辺機器や端末情報）との間の情報通信方式（ファイル転送プロトコル）の一つであるメディア・トランスファー・プロトコル（以下「ＭＴＰ」という。）に標準対応しているため、特別のアプリケーションを導入しないでも、ＭＴＰによる情報通信方式を使用する機器（以下「ＭＴＰデバイス」という。）との間で相互に情報通信をすることができる。

（甲２１、６７、７１、９８、乙４４、弁論の全趣旨）

⑷　Ａによる漏えい行為

ア　Ａは、平成２５年７月頃から平成２６年６月２７日までの間（以下「本件当時」という。）、多摩事務所において、①本件パソコンからバッチサーバを経由してサーバコンピュータに保存されている本件データベースにアクセスし、顧客情報を抽出する内容のＳＱＬ（データベースから必要な情報を抽出する条件等が記載されたプログラム）コマンドを入力して顧客情報を本件パソコンの画面上に表示させ（ただし、テラタームの画面を最小化して、パソコンの画面上からは見えないようにしていた。）、これを本件パソコンに保存した上で、②ＵＳＢケーブルを用いて、Ａが所有していたスマートフォン（以下「本件スマートフォン」という。）を本件パソコンのＵＳＢポートに接続し、上記①の顧客情報を本件パソコンから

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不正に取得した（以下「本件取得行為」という。）。

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。本件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、上記②のデータの転送は、ＭＴＰによって行われた。

（甲５、１７～１９、５３、６５、６６、８７、８８、弁論の全趣旨）

イ　Ａは、本件当時、本件取得行為によって取得した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（以下、この売却行為を「本件売却行為」といい、本件売却行為と本件取得行為を併せて「本件漏えい行為」という。）。

（争いがない。弁論の全趣旨）

ウ　Ａが本件取得行為により取得した顧客情報は、延べ約２億１６３９万件であり、約４８５８万人分の個人情報が含まれていた。

（争いがない）

エ　平成２７年３月３０日、警視庁生活経済課に対する取材に基づいて、Ａが本件取得行為によって取得した顧客情報は、本件売却行為の後、教育関連会社等約５００社に流出したとする報道がされた。

（甲５１）

⑸　本件漏えい行為の発覚及びその後の被告ベネッセＣｏの対応

ア　被告ベネッセＣｏは、平成２６年６月下旬、顧客から、被告ベネッセＣｏだけに登録した情報に基づいてダイレクトメールが届くなどの問合せが急増したことから、自社の顧客情報が社外に漏えいしている可能性を認識し、同月２７日に調査を開始するとともに、同月３０日には経済産業省に状況を報告して今後の対応を相談した。同社は、同年７月７日には上記漏えいを確認して警視庁に捜査を依頼し、これにより捜査が開始された。同

社は、同月１５日、警視庁に対してＡを刑事告訴した。

（甲５、２５、乙１７）

イ　被告ベネッセＣｏは、平成２６年７月９日、本件漏えい行為の概要を説明し、お詫びをするとともに今後の顧客への対応や再発防止策等について説明する目的で記者会見を実施し、その後も、事実関係が明らかになる都度、新たな情報をプレスリリースにより提供した。

また、被告ベネッセＣｏは、同月１２日以降、個人情報の漏えいの事実が確認された顧客ら（情報漏えい対象者本人又はその保護者）に対し、「お客様情報の漏えいについてお詫びとご説明」等と題する通知書（以下「本件通知書」という。）を送付し、その後、当該顧客らの選択に従って、①当該顧客らに対し、お詫びの品として５００円分の金券（選べる電子マネーギフト又は全国共通図書カード）を交付する方法、又は、②漏えい１件当たり５００円を「財団法人ベネッセこども基金」（被告ベネッセＣｏが本件漏えい行為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謝罪を行った。

さらに、被告ベネッセＣｏは、本件漏えい行為により漏えいした個人情報を利用していると考えられる業者に対し、利用停止や事実確認の働きかけを行った。

（甲１、５、２５、乙１、１７、２２、弁論の全趣旨）

⑹　本件当時の被告シンフォームにおける情報セキュリティの状況

ア　被告シンフォームは、本件当時、本件パソコンを含む業務用パソコンに、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）製の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、情報漏えい防止を目的とするものであり、すべてのデバイスについて接続（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み込み）を制御（禁止）することができる機能を有していた。

被告シンフォームは、本件当時、本件セキュリティソフトについて「リムーバブルメディア、ＣＤ／ＤＶＤ、外付けＨＤＤ」へのデータの書き出しのみを制御（禁止）する設定としていたため、マス・ストレージ・クラス（以下「ＭＳＣ」という。ＵＳＢメモリ等のＵＳＢ機器とパソコンとの間の通信方法である。ＵＳＢ機器は、Ｗｉｎｄｏｗｓによって「リムーバブルディスク」と認識される。）によるデータ通信に対してはデータの書き出しを制御（禁止）することができていたが、ＭＳＣとは異なる規格であるＭＴＰによるデータ通信（以下「ＭＴＰ通信」という。）に対してはデータの書き出しを制御（禁止）することができていなかった。

（甲１、５、２５、７１～７３、９６、乙４４、６８、７０、弁論の全趣旨）

イ　被告シンフォームは、本件当時、アラートシステム（データベースが保存されているサーバコンピュータと個別の業務用パソコン等との間の通信量を監視し、通信量が一定時間中に一定の基準値を超えた場合に、管理者に対してメールにより警告が発せられるものをいう。）を採用していたものの、本件データベースが保存されているサーバコンピュータに関しては、本件パソコンを含む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設定する措置を講じていなかった。

（甲１、５、２５、６７、弁論の全趣旨）

ウ　多摩事務所では、私物のスマートフォン（以下「私物スマートフォン」という。）について、執務室内への持込みや業務用パソコンに接続して充電することが許容されていた。

（甲１７、６５、６７、６８、弁論の全趣旨）

⑺　経済産業大臣の被告ベネッセＣｏに対する勧告等

ア　被告ベネッセＣｏは、平成２６年７月１０日、経済産業大臣から、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。）３２条に基づく報告を命じられ、平成２６年９月１７日、経済産業省に最終報告書を提出した。

経済産業大臣は、同月２６日、被告ベネッセＣｏに対し、被告ベネッセＣｏには、その顧客情報のシステム開発・運用に関する委託先である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等、委託先に対する必要かつ適切な監督を怠った個人情報保護法２２条違反の行為が認められるとして、個人情報保護法３４条１項に基づき、委託先の監督の徹底を勧告した。

（甲６、２５、弁論の全趣旨）

イ　一般財団法人日本情報経済社会推進協会は、平成２６年１１月２６日、被告ベネッセＣｏに対し、委託先の監督及び安全管理措置（資源、役割、責任及び権限を含む。）の両面において不備があったことや、漏えいした個人情報が膨大で、幼児や小中学生などの若年層の個人情報を多数含むため、長期にわたる影響が見過ごせないこと等を理由として、プライバシーマーク（上記協会が個人情報に対して適切な保護措置を行う体制を整備していることを独自に認定する制度であり、日本工業規格「ＪＩＳＱ１５００１個人情報保護マネジメントシステムー要求事項」に適合するか否かについて、民間事業者団体の指定機関が審査して、上記協会が付与しているもの）の付与を取り消す旨の発表をした。

（甲３３、弁論の全趣旨）

⑻　Ａの刑事事件

Ａは、平成２６年７月１７日、不正競争防止法違反の被疑事実に係る被疑者として逮捕された後、本件漏えい行為の一部につき、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に対し、懲役３年６月及び罰金３００万円の有罪判決を宣告したところ、Ａはこれを不服として控訴した。控訴審である東京高等裁判所は、平成２９年３月２１日、上記１審判決を破棄し、Ａに懲役２年６月及び罰金３００万円の有罪判決を宣告した。

（甲５、１７、２５、５３）

３　争点

⑴　訴訟代理権の欠缺

⑵　本件漏えい行為により原告らの個人情報が漏えいしたか。

⑶　本件漏えい行為について被告シンフォームに過失があるか。

⑷　本件漏えい行為について被告ベネッセＣｏに過失があるか。

⑸　被告ベネッセＣｏ及び被告シンフォームの行為に違法性が認められるか。

⑹　被告ベネッセＣｏは、被告シンフォームの不法行為について使用者責任を負うか。

⑺　被告シンフォームは、Ａの不法行為について使用者責任を負うか。

⑻　被告ベネッセＨＤは、不法行為責任を負うか。

⑼　本件漏えい行為により原告らに損害が発生したか及びその額

４　争点に関する当事者の主張

⑴　訴訟代理権の欠缺（本案前の答弁）について

【被告らの主張】

被告らは、本件訴訟係属後、原告らの訴訟委任状の不備を指摘し、原告らも指摘された不備を是正していたところであるが、少なくとも以下の原告らについては現時点においても不備が是正されていない。

訴訟委任状について、以下のア及びイの不備のある原告らについては、適法な訴訟委任の意思を確認できない以上、訴えが却下されるべきであり、以下のウ及びエの不備のある原告らについても、訴訟委任の意思を確認できな

い部分の訴えは却下されるべきである。

ア　法定代理人親権者２名の署名の筆跡及び押印の印影が同一の訴訟委任状

未成年者の法定代理人親権者が２名いる場合、原告ら訴訟代理人が訴訟追行について委任を受けるに当たっては、各法定代理人親権者から委任を受ける必要があり（民法８１８条３項）、訴訟代理人の権限は書面で証明しなければならない（民訴規則２３条１項）。

しかるに、少なくとも下記の原告らは、本件の訴訟委任状に係る法定代理人両名の署名の筆跡及び押印の印影が同一であり、少なくとも両名のいずれか一方については、自ら署名押印した事実が認められず、訴訟委任の意思が認められない。

記

原告番号１－１８０、同１－８２８、同１－８８７、同１－１０３４、同１－１１１７、同１－１２２８・１２２９、同１－１４５６、同１－１４６０、同１－１５３８、同１－１７４４・１７４５、同２－６、同２－７１、同２－３０１及び３０２、同２－６４１、同２－６９６、同３－１１７～１２０、同３－３６３、同３－４９７、同３－８０５～８０７、同３－８２５、同３－８４５・８４６、同４－８４・８５、同４－１１４・１１５、同４－５２９・５３０、同４－７５９・７６０、同４－１１０８、同４－１１５９、同４－１１６９

以上

イ　他の訴訟委任状における署名の筆跡及び押印の印影と同一の訴訟委任状

少なくとも下記の原告らは、本件の訴訟委任状に係る署名の筆跡及び押印の印影が、他の訴訟委任状における署名の筆跡及び押印の印影と同一であり、少なくともいずれか一方については、自ら署名押印した事実が認められず、訴訟委任の意思が認められない。

記

原告番号３－４８４と４８６、同４－６７１と６７２、同４－９６３と９６４

以上

ウ　捨印のない訴訟委任状

少なくとも下記の原告らは、本件の訴訟委任状に捨印が押印されていない。

そして、訴訟委任状で委任する事件の相手方欄には被告ベネッセＣｏのみが不動文字で印字されていることから、訴訟委任状作成後に相手方欄に「外」を加筆したり、被告ベネッセＨＤ又は被告シンフォームを追記した原告らについては、被告ベネッセＨＤ又は被告シンフォームを被告とする訴訟を委任したことが確認できない。

記

原告番号１－３３６・３３７、同１－３４２～３４４、同１－４４８、同１－４７６、同１－５０８、同１－５３５、同１－７１９、同１－７８６、同１－９６３、同１－１１７５、同１－１３２３・１３２４、同１－１３４６、同１－１４２７、同１－１５６８～１５７０、同１－１６０９、同２－３３、同２－６２５、同２－７９９、同２－８２７～８２９、同２－８５７・８５８、同２－９４４、同２－９９４・９９５、同２－１００２、同２－１０７８、同２－１０８１、同２－１１３２・１１３３、同２－１２２５、同２－１２６０・１２６１、同２－１２６８・１２６９、同２－１３４２、同２－１４５０・１４５１、同２－１４７４・１４７５、同２－１５９０、同３－１０７～１０９、同３－３００・３０１、同３－５１５

以上

エ　捨印はあるものの「外」が加筆されていない訴訟委任状

少なくとも下記の原告らは、本件の訴訟委任状に捨印はあるものの「外」

が加筆されていない。

そして、訴訟委任状で委任する事件の相手方欄には被告ベネッセＣｏのみが不動文字で印字されていることから、同原告らについては、被告ベネッセＨＤ又は被告シンフォームに対する訴訟を委任したとはいえない。

記

原告番号１－２１、同１－６９、同１－１５６、同１－１６７・１６８、同１－１７４、同１－１９８、同１－３０８、同１－３５８、同１－４６３、同１－４９５、同１－５８６、同１－６１０、同１－６２９・６３０、同１－６３２、同１－７５１、同１－７６１、同１－９２２、同１－９３０、同１－１０３９、同１－１０５７、同１－１１６３、同１－１２３４、同１－１３２９、同１－１３４８、同１－１５２９、同１－１７３４、同１－１７７２・１７７３、同３－４８５

以上

【原告らの主張】

ア　署名の筆跡及び押印の印影が同一であるとの主張について

署名の筆跡及び押印の印影が同一との点は、被告らの主観的判断にすぎず、否認する。

民訴規則２条１項によれば、訴訟委任状には「記名押印」が求められているにすぎず、そもそも自署は要件とされていない。また、「押印」についても本人のみが使用する印鑑を用いることを要求されているものではなく、同じ姓を持つ親族が共通の印鑑を用いることも何ら不合理ではない。

したがって、訴訟委任状の氏名の表記につき、印字若しくは他人が代筆した氏名が記載され、又は同じ姓の親族と同一の印鑑が使用されていたとしても、訴訟委任状の有効性は否定されない。

なお、原告ら訴訟代理人は、原告らから訴訟委任状を受領する際、意思確認のため、併せて本人確認書類の提出を受けており、本人の意思に基づ

き作成されたものであることは確認している。

イ　捨印がないか又は「外」が加筆されていない訴訟委任状

訴訟委任状の相手方欄については、被告となるべき者のすべてが正確に記載されていなければ委任の意思が確認できないものとして無効になるわけではない。

原告らは、本件漏えい行為によって責任を負うべき相手方に対する訴訟の提起を委任する意思を有し、原告ら訴訟代理人に訴訟委任状を提出したのであり、被告として被告ベネッセＣｏのみが記載された訴訟委任状であったとしても、「被告株式会社ベネッセコーポレーション　外」と記した訴訟委任状と同様に、被告らに対する訴訟委任状として有効である。

⑵　争点⑵（本件漏えい行為により原告らの個人情報が漏えいしたか。）について

【原告らの主張】

本件漏えい行為によって、被告ベネッセＣｏから、サービス登録者及び登録した保護者又は子の氏名、性別、生年月日、続柄、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、出産予定日が流出した（なお、クレジットカード番号についても当初流出した可能性があると公表されたが、被告ベネッセＣｏは後にクレジットカード番号の流出はなかったと発表している。）。

【被告らの主張】

ア　別紙７－１～５の各認否表（なお、取下げ済みの原告が含まれていることがある。以下、総称して、単に「別紙７認否表」という。）「情報項目」欄に「〇」の記載がある情報項目については、本件漏えい行為によって当該情報項目に関する漏えいがあったことを認める。

イ　別紙７認否表の「情報項目」欄に「△」の記載がある情報項目については、本件漏えい行為によって当該情報項目に関する漏えいがあったことは

認めるものの、本件漏えい行為によって漏えいした情報の内容と原告らの主張する情報の内容が一致するかどうかは知らない。なお、性別、電話番号及びメールアドレスの情報項目については、原告らが漏えいした情報の具体的内容を主張しないため、当該情報項目の漏えいが認められる場合は、「△」を記載している。

ウ　別紙７認否表の「情報項目」欄に「▲」の記載がある情報項目については、本件漏えい行為によって当該情報項目に関する漏えいがあったことは認めるが、その具体的内容については、「備考」欄に記載の理由により、漏えいした情報の内容と原告らの主張する情報の内容が一致することを否認する。

エ　なお、別紙７認否表の「登録コードが原告のものかどうか」欄に「不明」の記載がある原告の「情報項目」欄に「△」の記載がある情報項目については、本件漏えい行為によって当該登録コードから導かれる人物（対応する原告であるか否かは不知）の当該情報項目に関する漏えいがあったことは認めるものの、本件漏えい行為によって漏えいした情報の内容と原告らの主張する情報の内容が一致するかどうかは知らない。

オ　別紙７認否表の「情報項目」欄に上記「○」、「△」及び「▲」の３つの印がいずれも記載されていない情報項目については、漏えいがあったことにつき否認し、又は漏えいがあったかどうかにつき知らない。

カ　原告らのクレジットカード情報が漏えいしたことは否認する。

⑶　争点⑶（本件漏えい行為について被告シンフォームに過失があるか。）について

【原告らの主張】

ア　予見可能性

以下の㋐～㋔の各事情からすれば、被告シンフォームは、本件当時、本件データベースにアクセスする権限を有する者において、ＵＳＢケーブル

を用いて私物スマートフォンを業務用パソコンのＵＳＢポートに接続し、業務用パソコンから私物スマートフォンにデータを転送する方法によって、業務用パソコンに保存された個人情報を不正に取得し得ることを予見することができた。

㈠ 以下の基準やガイドライン等の内容などからすれば、個人情報を取り扱う事業者にとって、本件当時、外部記録媒体へ格納する方法による情報漏えいのリスクや、これを防止するための対策の必要性等が広く認識されている状況にあった。

ａ 「情報システム安全対策基準」（平成７年通商産業省告示第５１８号により制定、平成９年通商産業省告示第５３６号により最終改正。以下「平成９年通産省基準」という。甲１４）には、「データ等は、機密度及び重要度に応じた区分を設け、保有、利用、配布、持出し、持込み、廃棄等の管理計画を策定すること」と記載されていた。

ｂ 「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「平成２１年経産省ガイドライン」という。甲１３）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、（中略）外部記録媒体を接続できないようにする。）」をすることが望ましいと記載されていた。

ｃ 独立行政法人情報処理推進機構（ＩＰＡ）の平成２５年３月２５日付け「組織における内部不正防止ガイドライン」（以下「平成２５年ＩＰＡガイドライン」という。甲４１）には、「重要情報を取り扱う業務フロア等の領域に個人の情報機器及び記録媒体を持ち込まれると、個人の情報機器や記録媒体に重要情報を格納して持ち出される恐れ」があることがリスクとして指摘されていたほか、重要情報を扱う物理

的区画内のセキュリティ強化策として、カメラ等で監視するとともに、監視している旨を伝えることが記載されていた。

d　日本工業標準調査会の平成１８年策定の「個人情報保護マネジメントシステムー要求事項（ＪＩＳ　Ｑ　１５００１：２００６）」（以下「ＪＩＳ基準」という。）及び財団法人日本情報処理開発協会（当時）の平成２２年9月１７日発行の「ＪＩＳ　Ｑ　１５００１：２００６をベースにした個人情報保護マネジメントシステム実施のためのガイドライン　第2版」（以下「平成２２年ＪＩＳガイドライン」という。甲２８）には、業務上の必要性に基づく限定対策として、個人情報の取得・入力及び利用・加工の各場面において、外部記録媒体を接続できないようにすることが掲げられていた。

e　日本データセンター協会の平成２５年8月２８日付け「データセンター　セキュリティ　ガイドブックＶｅｒ１．０」（以下「平成２５年データセンターガイドブック」という。甲２６）には、セキュリティ対策として、ＵＳＢメモリ等の外部記録媒体や携帯電話の持込み・持ち出し制限及び画像監視システムが記載されていた。

f　一般社団法人日本スマートフォンセキュリティフォーラム（ＪＳＳＥＣ）は、平成２４年１０月２６日付け「スマートフォン&タブレットの業務利用に関するセキュリティガイドライン」（以下「平成２４年セキュリティガイドライン」という。甲１１１）において、スマートフォンを「ＰＣにＵＳＢケーブルで接続し充電することによる不正な情報流出等も考えられます。」と指摘していた。

(イ)　Ａが本件取得行為を行った際に使用した本件スマートフォンは、平成２４年１２月頃に発売が開始された、ＭＴＰ通信に対応したスマートフォン（以下「ＭＴＰ対応スマートフォン」という。甲１９）であった。

スマートフォンやタブレット端末向けのＯＳのうち、Ｇｏｏｇｌｅが

提供するＡｎｄｒｏｉｄをＯＳとするスマートフォン（以下「Ａｎｄｒｏｉｄスマートフォン」という。）のうち、同年夏以降に発売されたものは、全てＭＴＰ通信に対応したバージョン４．０（以下「Ａｎｄｒｏｉｄ４．０」という。）以降のものであった。

また、Ａｎｄｒｏｉｄ４．０より前のバージョンをＯＳとするＡｎｄｒｏｉｄスマートフォンについては、電気通信事業者から、同年７月以降の一定期間、ＯＳをＡｎｄｒｏｉｄ４．０へバージョンアップするサービスが提供された。

平成２５年７月から同年９月までの期間と、平成２６年７月から同年９月までの期間における、日本国内におけるＡｐｐｌｅ Ｉｎｃ．が提供するｉＯＳ（ＭＴＰ通信に対応していなかった。）とＡｎｄｒｏｉｄのそれぞれのシェアを比べると、後者の方が大きく、Ａｎｄｒｏｉｄスマートフォンのうち、Ａｎｄｒｏｉｄ４．０以降のもの（ＭＴＰ通信に対応している。）は、平成２５年４月には広く普及していた。

㈣ ＭＴＰデバイスは、スマートフォン以外にも多岐にわたっており、本件当時の代表的な商用デバイス用のセキュリティソフトウェアは、既に平成１９年７月から平成２５年８月にかけて、ＭＴＰデバイスをウィンドウズ・ポータブル・デバイス（以下「ＷＰＤ」という。）等として制御の対象とする機能を有していた。このことは、ＷＰＤからの情報漏えいの危険性が広く認識されていたことを示している。

㈤ 被告シンフォームでは、業務用パソコンから本件データベースにアクセスする方法として、フリーソフトを使用してバッチサーバ経由でアクセスする方法があったが、ＩＤ及びパスワードを教示されている者であれば、上記の方法で本件データベースにアクセスし、本件データベースの個人情報を私物スマートフォン等に書き出すことは容易であった。

㈥ 被告シンフォームは、毎年実施する被告シンフォーム及び業務委託先

の従業員全員を対象とする情報セキュリティ研修において、顧客の個人情報の大量持ち出し事例の紹介やスマートフォンを含む外部記録媒体への書き出し制御を実施している旨を周知していたから、スマートフォンが外部記録媒体として機能することや私物スマートフォンへ個人情報を書き出す手法による情報漏えいのリスクを十分に把握していたといえる。

イ　私物スマートフォン等の持込禁止措置義務違反

㈠　以下のａ～ｄの各事情からすれば、被告シンフォームは、本件当時、業務委託先を含めた従業員による私物スマートフォン等の執務室への持込みを禁止する措置を講ずるべき注意義務（以下「持込禁止措置義務」という。）を負っていたというべきである。

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

ｂ　平成９年通産省基準は、情報システムの機密性を確保することを目的として、故意・過失による情報漏えいのリスクを未然に防止するために、情報システムの利用者が実施する対策項目を列挙したものであることからすれば、個人情報を取り扱う企業にとっての注意義務の最低限の水準となり、不法行為上の注意義務の基準となるというべきである。平成９年通産省基準には「データ等は、機密度及び重要度に応じた区分を設け、保有、利用、配布、持出し、持込み、廃棄等の管理計画を策定すること」と明記されている。

平成２５年ＩＰＡガイドラインは、企業等において必要な内部不正対策を効果的に実施することを可能とすることを目的とするものであ

るから、平成２５年ＩＰＡガイドラインで要求する事項を考慮しない場合には、不法行為上の注意義務違反となるというべきである。平成２５年ＩＰＡガイドラインは、個人の情報機器や外部記録媒体に重要情報を格納して持ち出されるおそれがあることをリスクとして指摘し、「個人のノートＰＣやスマートデバイス等のモバイル機器及び携帯可能なＵＳＢメモリ等の外部記録媒体の業務利用及び持込を制限しなければならない。」と定めている。

平成２５年データセンターガイドブックは、データセンターの適切なセキュリティに関する理解を深め、日本におけるデータセンターの活用のために広く参照されることを目標として、適切なセキュリティを示すものであり、当該基準は、個人情報を取り扱う企業にとっての注意義務の指標となる。平成２５年データセンターガイドブックには、ＵＳＢメモリ等の外部記録媒体や携帯電話の持込み・持ち出し制限がセキュリティ対策として挙げられている。

ｃ　被告シンフォームにおいて、私物スマートフォン等を業務上利用する必要はなく、この持込みを制限することには、コストも手間もかからない。

ｄ　被告シンフォームが執務室への私物スマートフォン等の持込みを禁止していれば、本件取得行為を防ぐことができた。

(ｲ)　被告シンフォームは、本件当時、私物スマートフォン等の業務エリアへの持込みを禁止していなかったのであるから、持込禁止措置義務違反がある。

ウ　業務用パソコンに対するＵＳＢ接続禁止措置義務違反

(ｱ)　以下のａ～ｅの各事情からすれば、被告シンフォームは、本件当時、業務用パソコンのＵＳＢポートを物理的にふさいだり、業務用パソコンのＵＳＢポートに私物スマートフォンを接続することを禁止するルール

を設けたりするなどして、業務用パソコンのＵＳＢポートに私物スマートフォンを接続することを禁止する措置を講ずるべき注意義務（以下「ＵＳＢ接続禁止措置義務」という。）を負っていたというべきである。

ａ　被告シンフォームは、前記イ(ア)ａのとおり、大量のセンシティブな情報を扱っているのであるから、被告シンフォームには、個人情報が漏えいしないように最大限の配慮をすることが求められる。

ｂ　平成２１年経産省ガイドライン（甲１３）は、経済産業分野における事業者等が行う個人情報の適正な取扱いの確保に関する活動を支援する具体的な指針として定められたものであり、「しなければならない」と記載されている規定は、それに違反すると経済産業大臣により個人情報保護法違反と判断され得るものとされ、「望ましい」と記載されている規定は、それに違反しても個人情報保護法違反と判断されることはないが、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れているとされている。なお、個人情報保護法は、個人情報の取扱いに関して事業者に注意義務を課すことによって、各個人の権利を保護するために定められた法律であり、同法が行政法規であるとしても、同法上の義務は、個人の権利を擁護することを目的として規定されているのであるから、不法行為上の注意義務となり得るといえる。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」において「外部記録媒体」を接続することができないようにすることが望ましいとの記載がされている。

平成２５年ＩＰＡガイドラインでは、組織内部者の不正行為による情報セキュリティ上のインシデントの発生が指摘され、内部不正の防止に対する取組を推進すべきとされている（甲４１）。

ＪＩＳ基準は、事業者が業務上取り扱う個人情報を安全で適切に管理するための標準となるべく策定された日本工業規格であり、平成２

２年ＪＩＳガイドラインは、ＪＩＳ基準により個人情報保護マネジメントシステムを構築し、運用するためのガイドラインとして作成されたものである（甲２８）。したがって、ＪＩＳ基準等で要求されている事項を満たさない場合には、業務上個人情報を取り扱う事業者に要求される水準を満たさないものとして、不法行為上の注意義務違反となる。平成２２年ＪＩＳガイドラインは、外部記録媒体を接続することができないようにすることを業務上の必要性に基づく対策として挙げている。

ｃ　ＵＳＢポートを物理的にふさぐ器具は、遅くとも平成１７年には発売され、情報漏えい対策として一般的なものとなっていた（甲２３、２４）。

ｄ　被告シンフォームにおいて、私物スマートフォンを業務用パソコンのＵＳＢポートに接続する業務上の必要性はなく、ＵＳＢポートを物理的にふさぎ、又は少なくとも接続を禁止するルールを設けることには、コストも手間もかからない。業務への支障についても、必要に応じて、一時的に上司等の立会いの下、ＵＳＢメモリの接続を認めれば、支障はない。

ｅ　被告シンフォームにおいて、業務用パソコンのＵＳＢポートに私物スマートフォンを接続することを禁止していれば、本件取得行為を防ぐことができた。

㈠　被告シンフォームは、本件当時、業務用パソコンのＵＳＢポートにスマートフォンを接続することを禁止する措置を講じていなかったのであるから、ＵＳＢ接続禁止措置義務違反がある。

エ　情報書き出し制御措置義務違反

㈠　以下のａ～ｅの各事情からすれば、被告シンフォームは、本件当時、ＭＴＰ通信に対し、①パソコンからデバイスへのデータの書き出しのみ

を制御（禁止）する機能、又は、②接続制御機能〔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み込みのいずれも制御（禁止）する機能をいう。〕を備えたセキュリティソフトを業務用パソコンに搭載することにより、ＭＴＰ通信による業務用パソコンからデバイスへの情報の書き出しを制御（禁止）する措置を講ずるべき注意義務（以下「情報書き出し制御措置義務」という。）を負っていたというべきである。

ａ　被告シンフォームは、前記イ㋐ａのとおり、大量のセンシティブな情報を扱っているのであるから、被告シンフォームには、個人情報が漏えいしないように最大限の配慮をすることが求められる。

ｂ　平成２５年ＩＰＡガイドラインには、個人の情報機器及び外部記録媒体が持ち込まれた場合の情報持ち出しのリスクが具体的に指摘されている（甲４１）。

ｃ　前記ア㋑のとおり、平成２４年夏以降に発売されたＡｎｄｒｏｉｄスマートフォンは、全てＭＴＰ通信に対応したＡｎｄｒｏｉｄ４．０以降のものであり（甲５２）、相当程度普及する見通しであったから、それを予測することができる時点で、その対策が当然に必要となる。

ｄ　前記ア㋒のとおり、代表的な商用デバイス用のセキュリティソフトウェアは、平成１９年７月から平成２５年８月にかけて、ＭＴＰ通信に対応していた。

ｅ　業務用パソコンに搭載されたＭＴＰ通信に対する書き出し制御機能又は接続制御機能を備えたセキュリティソフトウェアの設定を、ＷＰＤについて接続を制御する設定に変更することは、業務用パソコンからＭＴＰ対応スマートフォンを利用した情報漏えいを防止する最も効果的な方法であった。

㋑　被告シンフォームは、本件当時、業務用パソコンにＷＰＤを接続する

業務上の必要性がないにもかかわらず、本件セキュリティソフトのＷＰＤに対する接続制御機能を無効とする設定にしていた（甲７３）ため、本件取得行為が可能になったのであるから、被告シンフォームには、情報書き出し制御措置義務違反がある。

【被告シンフォームの主張】

ア　予見可能性について

以下の㋐、㋑の各事情からすれば、被告シンフォームは、本件当時、本件データベースにアクセスする権限を有する者において、ＵＳＢケーブルを用いて、ＭＴＰ対応スマートフォンを業務用パソコンに接続し、ＭＴＰ通信により業務用パソコンから私物スマートフォンにデータを転送する方法によって、業務用パソコンに保存された個人情報を不正に取得し得ることを予見することができたとはいえない。

㋐　被告シンフォームは、外部記録媒体に情報を書き出すことを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。

㋑ａ　本件当時まで、①ＭＴＰ通信によりパソコンからスマートフォンにデータが書き出されることによる情報の流出の危険性や、②ＭＴＰ通信による情報の流出につき、ＭＳＣによる情報通信方式を使用する機器（以下「ＭＳＣデバイス」という。）を制御する従来の技術的措置とは異なる対策を採らなければならない必要性は、社会的に認識されていなかった。そして、本件当時は、パソコンからスマートフォンに業務上の文字情報ファイル（テキストファイルやドキュメントファイル）を転送する場合には、スマートフォンはパソコンからＭＳＣデバイスである「リムーバブルメディア」として認識されるため、ＭＳＣによるデータ通信（以下「ＭＳＣ通信」という。）を正しく制御して

いれば、パソコンからスマートフォンへの文字情報ファイルの転送を制御することができるものと認識されていた。

b　本件当時までに、業務用パソコンからスマートフォンにデータの書き出しがされて外部に情報が持ち出されるなど、ＭＳＣデバイスに対する書き出し制御措置がスマートフォンに対しては機能しない事態があることを疑わせる事故やトラブルが発生したことはなく、被告シンフォームにおいて、そのような事態が生じ得ることにつき疑いを抱く契機はなかった（乙１５、４４、５２、６８等の専門家意見書も同旨）。

c　さらに、本件当時の情報セキュリティ対策の一般的知見において、ＷＰＤに対する通信を制御することによってスマートフォンとの間の通信をも制御するとの発想はなく、本件セキュリティソフトにおいても、本件当時、ＷＰＤに対する接続を制御することによって、スマートフォンとの間の通信を制御することを想定した仕様にはなっていなかった。本件セキュリティソフトにおいて、スマートフォンの機種によって認識されるデバイスの種別（「リムーバブルメディア」か「ＷＰＤ」か）が異なることが判明したのは、本件漏えい行為が発覚した後である。

イ　個人情報保護法違反等の位置づけ

本件は、専門性を有し、日々技術的進展のある情報セキュリティ分野での一定時点における作為義務の有無が問題となる事案であるから、回避義務違反の存否は、経産省ガイドラインにおいて「しなければならない」（義務的事項）とされている対策及びこれと同視し得る通常の事業者において一般的にとるべきと考えられていた対策（標準的対策）を講じていたか否かを基準として判断されなければならない。

個人情報保護法は、個人の権利利益の保護等の目的で、予防的に、一定

の名宛人について公法上の安全管理措置義務を定めるものであって、同法に定める義務に違反したからといって、直ちに不法行為上の過失があることになるものではない。また、原告らの指摘する各種ガイドライン等も、以下の㋐～㋓のとおり、本件における被告シンフォームの注意義務を根拠付けるものではない。

㋐　平成２１年経産省ガイドラインは、個人情報保護法を踏まえ、また個人情報保護法８条に基づき個人情報保護法に定める事項に関して必要な事項を定め、経済産業分野における事業者等が行う個人情報の適正な取扱いの確保に関する活動を支援する具体的な指針として定められているものであり、平成２１年経産省ガイドラインの違反は、個人情報保護法違反にはなり得るが、不法行為上の過失に結びつくものではない。

㋑　平成９年通産省基準は、スマートフォンが市場に流通する以前の基準であって、平成９年に改正された後、本件当時まで改正されておらず、これが制定された当時と本件当時とでは、情報システムに関する技術や、これを取り巻く環境が全く異なっていたことからすれば、平成９年通産省基準は、本件当時の情報システムに当てはめ得るものではなく、情報セキュリティ対策の基準としての有用性は既に失われていたのであり、その後平成２１年経産省ガイドラインが作成されたことなどから、本件当時、情報セキュリティの分野において平成９年通産省基準を参照する必要はなくなっており、実務上も参照されていなかった。また、平成９年通産省基準は、サーバルームやデータセンター（様々な情報通信機器を設置・運営することに特化した建物と設備の総称）におけるセキュリティ対策に係る基準であって、通常の企業の執務室における情報セキュリティ対策に当てはめることは不適当である。

㋒　平成２５年ＩＰＡガイドラインは、組織における内部不正を防止するためのノウハウ集にすぎず、違法とはいえない行為も対象に含めて防止

策を提示するものである。同ガイドラインは、重要な情報が直接格納されているサーバの存在するサーバルームでは、外部記録媒体を直接サーバ等の機器に接続することが可能であって情報漏えいの危険性が極めて高い一方で、サーバルームでは通常の業務を行うことは基本的に考えられないことを踏まえ、端末や記録媒体等の持込を制限すべきとするものとしたものである。

被告シンフォームの執務室は、重要情報の格納サーバなどは設置されておらず、通常の業務が行われていたのであるから、平成２５年ＩＰＡガイドラインを本件に適用できないことは明らかである。

㈡　ＪＩＳ基準等は、事業者が、法律への適合性はもとより、自主的により高いレベルの個人情報保護マネジメントシステムを確立し運用していることをアピールできるという趣旨の任意基準であり、個人情報保護法の要求水準を超えた高い保護レベルを前提としている。

㈢　平成２５年データセンターガイドブックは、データセンターを対象としており、企業の日常業務が行われる執務室における情報セキュリティ対策の基準としては不適当である。

ウ　私物スマートフォン等の持込禁止措置義務違反について

以下の㈠～㈡の各事情からすれば、被告シンフォームは、本件当時、私物スマートフォン等の持込禁止措置義務を負っていたとはいえず、被告シンフォームに義務違反はない。

㈠　保管されている個人情報の多寡や当該個人情報の対象者の属性によって、とるべき安全管理措置の水準が異なる理由はない。

㈡　前記イのとおり、平成９年通産省基準の記載、平成２５年ＩＰＡガイドラインの記載及び平成２５年データセンターガイドブックの記載は、被告シンフォームの注意義務を根拠付けるものとはならない。

㈢　平成２１年経産省ガイドラインでは、私物スマートフォン等の持込禁

止は、義務的事項とも、望ましい事項ともされていない。

なお、本件漏えい行為が発覚した後も、私物スマートフォン等の持込禁止は、プライバシーマークやＩＳＭＳ認証（情報セキュリティに関する国際規格の１つであるＩＳＭＳ認証基準に適合していることを示す第三者機関による認証をいう。以下同じ。）を取得しようとする企業でも、標準的に採用されている措置ではなかった。

㈎　私物スマートフォンの持込みの禁止は、これを徹底しない限り実効性がない一方、これを徹底すると業務を著しく阻害することとなり、現実的ではない。かえって、平成２５年頃には、従業員が私物のＩＴ機器（スマートフォン等）を職場内に持ち込んで業務に利用することはむしろメリットのあるものとして肯定的に受け止められてさえいたのであり（乙４４）、本件当時に私物スマートフォンの職場への持込みを禁止することが標準的な措置ということはあり得ない。

エ　業務用パソコンに対するＵＳＢ接続禁止措置義務違反について

以下の㈀～㈁の各事情からすれば、被告シンフォームは、本件当時、ＵＳＢ接続禁止措置義務を負っていたとはいえず、被告シンフォームに義務違反はない。

㈀　平成２１年経産省ガイドラインには、本件当時、業務用パソコンに対するＵＳＢ接続禁止措置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。原告らの指摘する平成２１年経産省ガイドラインの該当部分は、「個人データを入力できる端末」、すなわち、個人データを入力すること（のみ）を目的とする端末について「外部記録媒体」を接続することを対象とした記載であるのに対し、本件パソコンは、個人データの一時記録も含め、広く本件システムの開発及び運用業務に使用されていたのであるから、上記端末には該当しない。また、スマートフォンは、「外部記録媒体」とは異なる

ものとして扱われている。

㈠　平成２５年ＩＰＡガイドラインは、組織内部者の不正行為による情報セキュリティ上のインシデントが発生している点について、「ＩＰＡは、・・・今後も組織における内部不正の防止に向けた取り組みを推進していきます。」と記載しているが、このような記載があるからといって業務用パソコンに対するＵＳＢ接続禁止措置義務を根拠付けるものとはならない。

㈡　平成２２年ＪＩＳ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。したがって、平成２２年ＪＩＳガイドラインの記載は、被告シンフォームの注意義務を根拠付けるものとはならない。

㈢　本件当時、業務上利用するパソコンに対するＵＳＢ接続禁止措置を講じている企業は少なかったのみならず、その後も、プライバシーマークやＩＳＭＳ認証を取得しようとする企業においても、同措置を講じていた会社は数％程度しかなく、その他の企業では同措置を採用していないのであるから、同措置は標準的に採用されていた措置ではなかった。

㈣　ＵＳＢポートを物理的にふさぐ器具は取り外し可能であり、また、パソコンには、マウス、キーボード及び業務上利用するＵＳＢなどを接続するためにＵＳＢポートが必要であって、全てのＵＳＢポートをふさぐことはできないのであるから、ＵＳＢポートをふさぐことは、本件取得行為に対する有効な対策とはならない。

オ　情報書き出し制御措置義務違反について

以下の㈠～㈢の各事情からすれば、被告シンフォームは、本件当時、情報書き出し制御措置義務を負っていたとはいえない。したがって、被告シンフォームには、情報書き出し制御措置義務違反はない。

㈠　平成２１年経産省ガイドラインは、情報書き出し制御措置につき、義

務的事項とも、望ましい事項ともしておらず、平成２５年ＩＰＡガイドラインも、情報書き出し制御措置に言及していない。

㈠　情報書き出し制御措置は高度な対策であり、一般の企業に求めることは現実的でなく、プライバシーマークやＩＳＭＳ認証を取得しようとする企業においても、書き出し制御措置を採用していない企業の方が多く、標準的に採用されていた措置ではなかった。

㈡　情報書き出し制御措置を採っている少数の企業でも、ＭＴＰ通信を対象としていたものはほとんどなく、ＭＴＰ通信に対する情報書き出し制御措置は標準的に採用された措置ではなかった。

㈢　被告シンフォームは、平成２３年夏から、業務用パソコンに、外部記録媒体に情報を書き出すことを制限する本件セキュリティソフトを搭載していたところ、本件取得行為が発覚するまでは、そもそもスマートフォンからの情報漏えいリスク自体想定されていなかったのであり、さらに、ＭＴＰ対応スマートフォンによる情報漏えいリスクについては、情報セキュリティの専門家すらもほとんど認識しておらず、メーカー等からの注意喚起もされていなかった。被告シンフォームの業務用パソコンから外部記録媒体への情報書き出しが制御されていないことを疑わせる事故等が生じたことはなく、このような報告がされることもなかった。

なお、ＭＴＰデバイスはパソコンから「ＷＰＤ」と認識されるところ、本件セキュリティソフトは、ＷＰＤに対する接続制御機能を有していたが、本件漏えい行為以前に、本件セキュリティソフトのパンフレットその他のマニュアル等を含む一切の資料において、ＵＳＢ接続されたスマートフォンに対するデータの転送を防止するためには「ポータブルデバイス」（ＷＰＤ）を使用不可能とする設定をしなければならない旨の記載はなかったのであり、「ＭＴＰ」、「ＭＳＣ」という通信方式に関する言及すら皆無であった。したがって、被告シンフォ

ームにおいて、本件セキュリティソフトの設定を変更しＭＴＰの通信方式に対応したスマートフォンへのデータ転送を阻止するために、「ポータブルデバイス」（ＷＰＤ）を使用不可能とする設定をする必要があるとの認識に至ることはできなかった。

そして、一般の企業における業務と同様に、被告シンフォームの業務においても、デジタルカメラ、デジタルビデオカメラ又はボイスレコーダーに記録された画像、動画及び音源を業務用パソコンに取り込むことは日常的に行われており、業務用パソコンにＷＰＤを接続する業務上の必要があった。

⑷　争点⑷（本件漏えい行為について被告ベネッセＣｏに過失があるか。）について

【原告らの主張】

ア　予見可能性

被告ベネッセＣｏが、本件当時、本件データベースにアクセスする権限を有する者において、ＵＳＢケーブルを用いて私物スマートフォンを業務用パソコンのＵＳＢポートに接続し、業務用パソコンから私物スマートフォンにデータを転送する方法によって、業務用パソコンに保存された個人情報を不正に取得し得ることを予見することができたことは、争点⑶に関する【原告らの主張】アと同様である。

イ　委託先の選定及び監督に関する注意義務違反

㋐　以下のａ～ｃの各事情からすれば、被告ベネッセＣｏは、本件当時、本件業務の委託先を選定するに当たり、適切に個人情報を管理する体制を備えた業者を選定するべき注意義務及び委託先において個人情報保護法２０条に基づく安全管理措置が適切に実施されているかを監督するべき注意義務（以下「委託先選定監督義務」という。）を負っていたというべきである。

ａ　個人情報保護法において個人情報を取り扱う事業者に求められる義務は、不法行為上の注意義務になるところ、個人情報保護法２２条は、同事業者が、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託し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。そして、平成２１年経産省ガイドラインには、「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及び委託先に委託された個人データの取扱いの状況を把握することが含まれると記載されている。

ｂ　ＪＩＳ基準には、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と、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旨が規定されている。

ｃ　被告ベネッセＣｏが取得した個人情報には、争点⑶に関する【原告らの主張】イ㋐ａのとおり、大量のセンシティブな情報が含まれていた。

㋑　被告ベネッセＣｏは、本件当時、本件業務の委託先として、適切に個人情報を管理する体制にある業者を選定しなかった。

また、被告ベネッセＣｏは、被告シンフォームに対して定期的に監査を行っていたが、本件セキュリティソフトにより情報書き出し制御がされているものと軽信して、被告シンフォームが私物スマートフォンを業務用パソコンのＵＳＢポートに接続することを禁止していないことを問題視することなく、また、本件セキュリティソフトの設定を監査対象としなかったなど、委託先において個人情報保護法２０条に基づく安全管

理措置が適切に実施されているかを監督していなかった。

したがって、被告ベネッセＣｏには、委託先選定監督義務違反がある。

【被告ベネッセＣｏの主張】

ア　予見可能性について

被告ベネッセＣｏが、本件当時、本件データベースにアクセスする権限を有する者において、ＵＳＢケーブルを用いて、ＭＴＰ対応の私物スマートフォンを業務用パソコンに接続し、ＭＴＰ通信により業務用パソコンから私物スマートフォンにデータを転送する方法によって、業務用パソコンに保存された個人情報を不正に取得し得ることを予見することができたとはいえないことは、争点⑶に関する【被告シンフォームの主張】アと同様であり、専門性・信頼性の高い委託先に本件業務を委託したにすぎない被告ベネッセＣｏにはより一層予見可能性がなかった。

イ　委託先の選定及び監督に関する注意義務違反について

以下の㋐～㋒の各事情からすれば、被告ベネッセＣｏには、業務委託先である被告シンフォームの選定及び監督につき、注意義務違反はない。

㋐　被告シンフォームは、争点⑶に関する【被告シンフォームの主張】のとおり、本件当時、高い水準の情報セキュリティ対策を講じており、原告ら主張の注意義務違反があったとはいえない。したがって、被告ベネッセＣｏには、被告シンフォームを本件業務の委託先として選定したことにつき、注意義務違反はない。

㋑　被告シンフォームでは、本件当時、情報セキュリティ及び個人情報保護において高度の情報セキュリティ対策・体制を備えていることが客観的に担保されており、製造、流通、ＥＣ又は金融の国内大手等の企業と比較しても遜色のない情報セキュリティの管理レベルにあった。

㋒　また、被告ベネッセＣｏは、本件当時、次のとおり、平成２１年経産省ガイドラインや情報セキュリティ対策の一般的な基準からしても、高

度な水準で被告シンフォームに対する監督を行っていた。

平成２１年経産省ガイドラインは、委託先から委託契約に盛り込んだ個人情報管理に関する事項の遵守に関する状況の全般についてチェックシート形式の書面等により定期的に報告を受けることを望ましい事項としているにとどまり、委託元において、委託先が採用している個別のセキュリティ対策を調査・検討し、業務委託先の採用していない他の考えられるセキュリティ対策を講ずることを求めることまでを、望ましい事項とはしていない。

被告ベネッセＣｏは、委託先である被告シンフォームに対する監督として、チェックシート方式の書面等による定期的な報告を求めることに加え、年に１回、監査の専門部署が２日ないし３日をかけて実地監査を実施していた。

被告らは、株式会社インターネットプライバシー研究所（以下「インターネットプライバシー研究所」という。）に対し、被告ベネッセＣｏが本件当時、被告シンフォームに対して実施していた監督が、当時の平成２１年経産省ガイドラインの「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、被告ベネッセＣｏが平成２６年当時実施していた被告シンフォームに対する監督は、上記ガイドライン「２－２－３－４．委託先の監督（法第２２条関連）」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施されていたことを確認している。

⑸　争点⑸（被告ベネッセＣｏ及び被告シンフォームの行為に違法性が認められるか。）について

【原告らの主張】

本件漏えい行為によって漏えいした個人情報は、無制限な開示、保有、利

用が許される情報ではなく、法的保護の対象となる。そして、本件漏えい行為に係る被告らの過失行為を正当化すべき理由は何らない。

本件漏えい行為に係る被告ベネッセＣｏ及び被告シンフォームの過失行為によって、原告らのプライバシーが侵害されたものであり、違法な権利侵害行為である。

【被告らの主張】

本件漏えい行為によって漏えいした個人情報は、社会生活を営む上で一定の範囲の他者に開示されることが当然に予定されている個人の識別などのための単純な情報にとどまり、また、当該情報は、名簿業者１社に売却されたにすぎない。

さらに、被告ベネッセＣｏ及び被告シンフォームは、本件漏えい行為を把握した後、速やかに対象となった顧客に謝罪し、個人情報が漏えいされた顧客一人当たり５００円相当の補償を実施し、再発防止のために、相当の費用及び労力をかけて対策を講じた。したがって、被告らの本件漏えい行為に係る行為は、社会通念上許容される限度を逸脱した違法な行為であるとはいえない。

⑹　争点⑹（被告ベネッセＣｏは、被告シンフォームの不法行為について使用者責任を負うか。）について

【原告らの主張】

ア　被告シンフォームの不法行為

被告シンフォームは、争点⑶に関する【原告らの主張】のとおり、持込禁止措置義務、ＵＳＢ接続禁止措置義務及び情報書き出し制御措置義務に違反して、原告らのプライバシーを違法に侵害したものであるから、原告らに対して不法行為責任を負う。

イ　事業執行性

本件システムは、被告ベネッセＣｏの商品・サービス開発やマーケティ

ングのために、被告ベネッセＣｏの保有する顧客情報を統合して分析に使用するためのシステムであり、その開発・運用・保守の業務（本件業務）は、被告ベネッセＣｏの「事業の執行」（民法７１５条１項本文）に該当するのであるから、前記アの被告シンフォームの過失行為は、被告ベネッセＣｏの「事業の執行について」（同項本文）されたものに該当する。

ウ　使用者性

以下の㋐～㋓の各事情からすれば、被告ベネッセＣｏは、本件業務について、被告シンフォームを実質的に指揮監督する関係にあったといえる。

㋐　被告ベネッセＣｏと被告シンフォームとの間の業務委託契約では、被告ベネッセＣｏが、被告シンフォームの安全管理措置について監督をすることや、被告シンフォームが受託業務を再委託する場合には事前に被告ベネッセＣｏの承諾を求めることが定められていた。

㋑　被告ベネッセＣｏは、被告シンフォームに対し、その従業員に対する研修等について指示を行っていた。

㋒　被告ベネッセＣｏは、月次で報告会を開催し、委託業務全般の進捗状況の確認を行うほか、規模の大きな開発・運用案件については週１回以上のペースで定例ミーティングを実施していた。そして、被告ベネッセＣｏは、本件システムの運用に当たり、動作状況を確認し、被告シンフォームに対し、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　被告ベネッセＣｏと被告シンフォームとは、現在は、被告ベネッセＨＤの１００％子会社同士の関係にあるが、もともとは、被告シンフォームは、被告ベネッセＣｏの１００％子会社であり、被告ベネッセＣｏの取締役又は監査役が被告シンフォームの役員に就任し、被告ベネッセＣｏにおける情報システム担当者が被告シンフォームのＩＴソリューション部の部長を兼任する関係にあった。

エ　まとめ

以上によれば、被告ベネッセＣｏは、原告らに対し、本件漏えい行為につき、被告シンフォームを被用者とする使用者責任を負う。

【被告ベネッセＣｏの主張】

ア　被告シンフォームの不法行為について

争点⑶に関する【被告シンフォームの主張】のとおり、被告シンフォームは、本件漏えい行為に関して不法行為責任を負わない。

イ　事業執行性について

被告シンフォームは、被告ベネッセＣｏとの間の業務委託契約に基づいて自らの「事業」として本件業務を行っていたものであり、被告シンフォームの行為が、被告ベネッセＣｏの「事業」（民法７１５条１項本文）の範囲に属していたとはいえない。

ウ　使用者性について

被告ベネッセＣｏが、被告シンフォームの従業員に対する研修等について指示をした事実はなく、被告シンフォームが被告ベネッセＣｏの１００％子会社であったこともない（そもそも親子会社であることは使用者性を裏付けるものではない。）。

被告ベネッセＣｏは、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ていたほか、委託業務の進捗を確認するなどしていたにすぎない。これらの事実は被告ベネッセＣｏの被告シンフォームに対する実質的指揮監督関係を基礎付けるものではなく、委託元が委託先に対して通常行う指図や情報交換にとどまる。

⑺　争点⑺（被告シンフォームは、Ａの不法行為について使用者責任を負うか。）について

【原告らの主張】

ア　Ａの不法行為

Ａは、本件漏えい行為により原告らに対して、不法行為責任を負う。

イ　事業執行性

本件取得行為は、Ａが、多摩事務所において、被告シンフォームの事業である本件業務を行う間に、被告シンフォームから貸与を受けた本件パソコンを使用して本件データベースにアクセスして行われたものである。Ａが、本件データベースへの広範なアクセス権限を付与され、その権限に基づいて行ったことからすれば、Ａの本件取得行為は、被告シンフォームの「事業の執行について」（民法７１５条１項本文）されたものといえる。

ウ　使用者性

被告シンフォームとＡとの間に直接の雇用関係はないものの、Ａは、被告シンフォームにおいて本件システムの開発、運用及び保守等を所管する顧客分析課に所属し、複数の個別案件を処理するグループに属し、被告シンフォームの社員であるグループリーダーが立案した計画、スケジュールに従って作業を行っていた。

そして、Ａに対して委託先の責任者とされる者は、平成２４年４月当初は毎日多摩事務所に来ていたものの、数か月後にはこれが週に２、３回となり、その後は一切多摩事務所に来なくなっていた。

このような事情からすれば、被告シンフォームは、本件業務について、Ａを実質的に指揮監督する関係にあったといえる。

エ　まとめ

以上によれば、被告シンフォームは、原告らに対し、本件漏えい行為につき、Ａを被用者とする使用者責任を負う。

被告シンフォームがＡの選任及びその事業の監督について相当の注意を払っていたとの被告シンフォームの主張は、争う。

【被告シンフォームの主張】

ア　事業執行性について

Ａによる本件取得行為は、「本件業務」そのものではない以上、同行為が本件業務中に行われたとしても、当然に業務の執行についてされたものとはいえない。

さらに、Ａは、被告シンフォームの従業員ではなく委託先会社（再委託先を含む。）における業務を行っていたものであり、Ａの行為が当然に被告シンフォームの「事業の執行について」（民法７１５条１項本文）行われたものとはいえない。

イ　使用者性について

被告シンフォームの社員は、緊急時の例外を除き、Ａに対し直接の指示をしたことはない。

また、Ａが、被告シンフォームの顧客分析課においてチーム（原告らはグループと呼称）に属していたのは、被告シンフォームが受託業務の内容・案件種別をチーム単位で割り振っていたためにすぎない。被告シンフォームは、受託した各業務をさらに再委託するという構造上、受託者の担当者たる被告シンフォームの社員がチームリーダーとなり、再委託先会社の計画をもとに、再委託先のリーダーと相談して案件を進めるという手順を採用していたから、チームリーダーである被告シンフォームの社員がＡ等の再委託先の要員に直接業務上の指示を出すことはなかった。

したがって、被告シンフォームとＡとの間に実質的な指揮監督関係は存在しない。

⑻　争点⑻（被告ベネッセＨＤは不法行為責任を負うか。）について

【原告らの主張】

ア　予見可能性

被告ベネッセＨＤが、本件当時、本件データベースにアクセスする権限を有する者において、ＵＳＢケーブルを用いて私物スマートフォンを業務用パソコンのＵＳＢポートに接続し、業務用パソコンから私物スマートフ

ォンにデータを転送する方法によって、業務用パソコンに保存された個人情報を不正に取得し得ることを予見することができたことは、争点⑶に関する【原告らの主張】アと同様である。

イ　個人情報の利用・管理に責任を持つ部門の設置義務違反

㋐　被告ベネッセＨＤは、純粋持株会社であって、子会社の株式を１００％保有し、その主たる業務は、子会社の支配・統括管理であって、その利益の源泉は子会社の事業活動に依存している。そして、純粋持株会社は、原則として対外的事業活動を行わないので、子会社に属する他の会社を支配し、これを統括管理することが取締役の基本的責務である。

被告ベネッセＨＤは、ベネッセグループを統括する会社として、個人情報保護の法制や平成２１年経産省ガイドラインの下、グループ全体について個人情報の管理体制を組織的に構築・運営し、合理的な安全対策を講ずべき義務を負っているのであり、併せて、同義務に基づき、完全子会社である被告ベネッセＣｏ及び被告シンフォームの情報管理につき、万全な指導監督を尽くすべき善管注意義務を負っている。

㋑　以下のａ～ｃの各事情からすれば、被告ベネッセＨＤは、本件当時、保有する個人情報の利用・管理に責任を持つ部門を自ら設置し、又は例えば被告ベネッセＣｏなどグループ内の企業に設置させるべき注意義務（以下「部門設置義務」という。）を負っていたというべきである。

ａ　争点⑶に関する【原告らの主張】ウ㋐ｂのとおり、個人情報保護法が定める義務は、不法行為上の注意義務を構成するところ、個人情報保護法２０条は、「個人情報取扱業務者は、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、個人情報を取り扱う事業者に対し、個人データの安全管理のために必要かつ適切な措置を講ずることを義務付けている。そして、平成２１年経産

省ガイドラインには、義務的事項として、個人データの安全管理措置を講ずるための組織体制の整備が挙げられている。

平成２５年ＩＰＡガイドラインには、「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」旨がリスクとして指摘されており、組織横断的な管理体制の構築として、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が求められている。

b　個人情報を取り扱うに当たり、利用・管理に責任を持つ部門が存在しない場合には、保有する情報を統括して管理することができず、個人情報の取扱いや管理が杜撰となり、情報の漏えいが生じる可能性が高まる。被告ベネッセＨＤ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であった。

c　被告ベネッセＨＤの完全子会社である被告ベネッセＣｏが取得した個人情報には、争点⑶に関する【原告らの主張】イ㋐ａのとおり、大量のセンシティブな情報が含まれていた上、被告ベネッセＣｏが被告シンフォームに本件システムの構築を委ね、被告シンフォームがその一部を他の業者に委託するなど、被告ベネッセＣｏの顧客情報に被告ら以外の会社の従業員が多数接触する状況であった。

㋒　被告ベネッセＨＤは、本件当時、保有する個人情報の利用・管理に責任を持つ部門を設置しておらず、グループ内の企業である被告ベネッセＣｏにも設置させていなかったため、個人情報の管理が不十分となっていた。

したがって、被告ベネッセＨＤには、部門設置義務違反がある。

【被告ベネッセＨＤの主張】

原告らの主張を踏まえても、個人情報を保有する被告ベネッセＣｏとは別法人である被告ベネッセＨＤが、いかなる理由で不法行為法上の注意義務として部門設置義務を負うこととなるのか不明であり、原告らの被告ベネッセＨＤに対する請求は主張自体失当というべきである。

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

⑼　争点⑼（本件漏えい行為により原告らに損害が発生したか及びその額）について

【原告らの主張】

本件で漏えいした個人情報は、被告ベネッセＣｏの公表によれば顧客情報３５０４万件分（重複分を除く実態件数約２８９５万件）とされており、流出した情報は、サービス登録者及び登録した保護者又は子の氏名、性別、生年月日、続柄、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、出産予定日である。当初はクレジットカード番号についても流出した可能性があると公表されており、原告らは自己のクレジットカードが使用されるかもしれないという不安感に怯えることとなった。

個人の氏名、住所、生年月日、電話番号、ファクシミリ番号、メールアドレスは、これらによって個人が識別され、個人の私生活の本拠に関わる情報及び個人を識別するために必要とされる情報として、私生活上の事実に関する情報である。これらの情報は、開示の必要性があり、開示した情報の管理について信頼できる範囲で開示するという性質のものであって、誰にでも開示してよいと考える者は稀である。また、出産予定日は特に親しい関係でなければ伝えない情報である。

しかも、被告ベネッセＣｏが保有・管理していたこれらの個人情報は、各個人というだけでなく、各世帯単位の情報が統合されているという点に特色があり、同情報を長期的に保管することによって各世帯における子の成長過程等が高度の確実さをもって予測可能となり、誘拐、「オレオレ詐欺」又は架空請求などに悪用される可能性がある、

さらに、本件の個人情報は、被告ベネッセＣｏが平成２６年１２月１５日に公表したものだけでも５２社へ拡散されており、これら以外にも拡散されていることが想定される。いったん流出した個人情報は、容易に複製され、数次の拡散が容易であり、そのすべてを消去することは不可能である。

実際に、原告らの中には、本件漏えい行為の後に、いわゆる迷惑メールやダイレクトメールの被害を受けている者もいる。

被告ベネッセＣｏは、本件漏えい行為の後に、顧客情報が流出した者に対し、謝罪の手紙及び５００円の金券を送付し、データ流出被害対策室を設置して２次被害対策を行ったとしているが、そうした措置によって拡散した情報がすべて消去されるわけではない。

以上の事情に加え、被告らの過失が重大であることなどを考慮すると、原告らの精神的苦痛に対する慰謝料額は少なくとも１人当たり５万円を下回ることはない。そして、訴訟提起に要した弁護士費用のうち上記損害と相当因果関係を有するものはその１割に相当する１人当たり５０００円とするのが相当である。

【被告らの主張】

ア　個人を特定し、識別するための基本情報にすぎないものは、その流出によっても、通常、平穏な日常生活や社会生活が害されるほどの精神的苦痛を受けるものではなく、その流出があったとしても、不法行為にいう「損害」には当たらない。

イ　原告らは、本件漏えい行為により、具体的・実質的損害を一切受けてお

らず、具体的・実質的損害が将来発生する蓋然性もなく、原告らが主張する損害は、抽象的な不安感、不快感又は個人情報の利用の可能性を内容とするものにすぎない。

本件の個人情報は、社会生活を営む上で開示を求められることが多い客観的な情報であるため、秘匿性が低く、その開示の相手方や予想される利用形態等に照らせば、原告らの不安感や不快感などの精神的負担も低いものにとどまる。本件の個人情報は、少なくとも名簿業者１社に売却されているものの、現代社会にあっては、名簿業者を利用した情報取得が広く一般に利用されており、誰でも各種の名簿に登載されていることが通常であるし、通常、自己の情報がいずれの名簿に登載されているかを確知することはできない。そして、住所、氏名、電話番号又はメールアドレスが名簿業者に漏えいしたことで想定される事態は、広告宣伝等のための文書送付、架電又はメール送付が行われるにとどまり、そういった広告宣伝等はそれ自体違法性のないごくありふれた行為である。

また、被告らは、意図的に本件の個人情報を開示したものではなく、むしろ、本件の個人情報が漏えいしないよう防御措置をとって厳重にその保護を図っていた上、本件情報漏えい発覚後も、事案の解明や再発防止策を講じたほか、情報漏えいの対象者に対して本件通知書を送付し、一人当たり５００円相当の補償を提供し、相談窓口の設置等を行い、情報拡散防止活動なども継続的に行ってきた。このような被告らの適切な対応により、原告らの精神的損害は慰謝されている。

仮に本件で顧客１人当たり５０００円の賠償義務があるとした場合、顧客４８５８万人分とすれば２４２９億円もの賠償金を支払うこととなるのであり、ひとたび大規模情報漏えい事故が発生すると当該企業の存続の途が絶たれることとなりかねず、社会に与える弊害は極めて重大である。

ウ　なお、姓や住所を変更した原告らについては、本件の個人情報から原告

らの氏名や住所を第三者に把握されることはないから、損害が認められる状況が既に解消されており、損害が認められないことはより一層明らかである。

第３　当裁判所の判断

１　争点⑴（訴訟代理権の欠缺）について

被告らは、一部原告らの訴訟委任状の不備を指摘した上で、当該原告らについては適法な訴訟委任の意思を確認できないとして、訴訟代理権の欠缺を主張している。

原告らは、被告らの指摘を受けて、当該原告らの訴訟委任状について一部は補正したものを提出したが、残りの原告らについては補正が未了である（弁論の全趣旨）。

被告らは、

ア　法定代理人親権者２名の署名の筆跡及び押印の印影が同一

イ　他の訴訟委任状における署名の筆跡及び押印の印影が同一

ウ　捨印のない訴訟委任状

エ　捨印はあるものの「外」が加筆されていない訴訟委任状

の４つの類型について訴訟代理権の欠缺を主張している。

しかしながら、民訴規則２条１項によれば、裁判所に提出すべき書面である訴訟委任状には「記名押印」が求められているにすぎず、自署は要件とされていないから、上記ア及びイについて問題となり得るのは押印の印影が同一であるという点にとどまる。訴訟委任状は訴訟代理権の存在を証する書面（民訴規則２３条１項）として提出されるものであって、当該訴訟を委任する意思を明らかにするための書面であるから、訴訟委任状への押印を通じて原告ら各人の委任の意思が示されていれば足り、原告ら各人が異なる印影を用いることは必須ではない。そして、原告ら訴訟代理人弁護士が、原告らから訴訟委任状を取り付ける際に、意思確認のために本人確認書類を徴求した

旨主張していることを考慮すると、既に提出済みの訴訟委任状によって原告らの委任の意思が示されているということができ、署名の筆跡及び押印の印影が同一又は類似しているとの理由でその意思が否定されるものではない。

上記ウ及びエについては、訴訟委任状の作成時点では相手方欄の記載の正確性を欠き（被告ベネッセＣｏのみを相手方欄に記載）、事後的に原告ら訴訟代理人弁護士において被告ベネッセＨＤ及び被告シンフォームを相手方欄に追記したが訴訟委任状には原告らが事後的な訂正を許容していたことを示す捨印やベネッセＣｏ以外にも被告とすることを示す「外」の記載がなかったことを指摘するものである。本件訴訟において、原告らは、本件漏えい行為によって責任を負うべき主体を被告として訴訟を行うことを原告ら訴訟代理人に委任していることが認められるところ（弁論の全趣旨）、いずれが訴訟の被告となり得るのかについては、原告らが直接顧客情報を提供した被告ベネッセＣｏについては当初から被告となるべきことが確定していたといえるが、その余の被告らについては、法人相互の関係性を精査しなければ法的責任の所在が判然としないことから、専門知識を有する原告ら訴訟代理人にその適切な選別を含めて委ねていたものと解することができる。そうすると、訴訟委任状に形式的に「外」や捨印がなかったとしても、原告らは当初から本件漏えい行為によって責任を負うべき主体を被告とした訴訟を委任する意思を有していたのであるから、被告ベネッセＣｏ以外の被告らに対する訴訟を委任する意思を有していたものというべきであって、原告ら訴訟代理人らによる追記があったとしても原告らの当初の委任の範囲内の事項にすぎないというべきである。

2　争点⑵（本件漏えい行為により原告らの個人情報が漏えいしたか。）について

別紙７認否表の「情報項目」欄に「○」、「△」又は「▲」の記載がある情報項目について、当該情報項目に関する漏えいがあったこと自体は、当事者間

に争いがない。

別紙７認否表の「情報項目」欄に「○」、「△」又は「▲」のいずれの記載もない空欄の情報項目については、当該情報項目の漏えいを基礎付けるに足りる証拠は提出されていないから、漏えいがあったと認めるに足りない。

なお、別紙７認否表の「情報項目」欄に「△」又は「▲」の記載のある情報項目については、それが原告らの主張する内容と一致するか否かについて争いがあるが、この点が結論に影響するか否かについては争点⑼において検討する。

３　認定事実

前記前提事実に加え、後掲各証拠（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、次の各事実を認めることができる。

⑴　Ａの多摩事務所における勤務状況

ア　被告シンフォームでは、事業開発本部の下部組織として事業開発部が設置され、事業開発部の中に顧客分析課が設置されており、本件業務を所管していたのは顧客分析課であった。

（甲６７、７５）

イ　顧客分析課は、多摩事務所において、本件業務等の業務を行っていた。平成２６年６月当時、顧客分析課には３９名が所属していたが、そのうち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、複数の委託先（１次委託先だけでなく、２次委託先等を含む。）の従業員であった。

顧客分析課の中には複数のチームが存在し、個別案件を効率的に進めるため各チームの中にさらに少人数で構成された複数のグループが編成され、各グループにはグループリーダーが置かれていた。グループリーダーは、常に被告シンフォームの従業員が担当し、具体的な作業工程を管理していた。

各グループでは、毎日又は毎週、進捗会議と呼ばれる打合せが行われ、当該グループのメンバー全員が参加し、前日の作業状況や当日の予定等を

話し合い、作業の進捗状況を共有していた。

（甲６５、６７、６８、７５）

ウ　被告シンフォームは、委託を受けた業務を、更に複数の業者に対して再委託することがあった。Ａは、システムエンジニアであり、本件業務について、被告シンフォームからみて３次委託先（被告ベネッセＣｏからみると４次委託先）の法人の従業員であった。Ａは、平成２４年４月から、被告シンフォームの多摩事務所の執務室において就労するようになり、顧客分析課の開発チームの中のグループに属して本件業務に従事していた。

（甲２５、６５、７５、８７、８８）

エ　Ａは、被告シンフォームの業務に従事するに当たり、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したり漏えいしたり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」の提出を求められ、これを提出するとともに、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ており、業務に従事するようになった後も、年１回実施される情報セキュリティ研修を受けていた。

（甲２５、６５、６８、８８）

オ　Ａは、被告シンフォームの従業員から、終業時刻近くに作業を依頼されたり、終業時刻後に開始される打合せに出席するように依頼されたりするなど、残業の指示を受けることがあり、それに応じていた。

Ａは、１次委託先に自己の労働時間を報告するほか、被告シンフォームに対しても、残業時間を含む労働時間を報告しており、被告シンフォームにおいてもＡの労働時間を把握していた。

Ａは、本件業務のほか、集計業務（被告ベネッセＣｏから、一定の条件に適合する契約を締結している顧客等のリストが欲しいとの要望があった際に、そのリストを提供する作業）やＱＡ業務（本件システムのユーザーである被告ベネッセＣｏの事業部からの分析ツールの使い方等の問合せに

対して回答を行う業務）も行っていた。ＱＡ業務については、被告ベネッセＣｏの担当者からＡの所属するグループのグループリーダー（被告シンフォームの従業員）とＡの両方に対してメールで問合せがあった際、Ａが、グループリーダーから指示を受けて、Ａにおいて被告ベネッセＣｏの担当者に対して直接回答することがあった。

平成２６年６月頃、被告シンフォームが被告ベネッセＣｏに対して作業内容や作業予定を報告し、問題点に関して質疑応答を行う内容の進捗会議が週に１回開催されていたところ、Ａは、グループリーダーからの指示で、グループリーダーと共に上記会議に参加し、議事録を起案したことがあった。

（甲６５、６６、６８）

カ　本件システムは、平成２４年４月に開発が始まり、平成２５年４月から一部について運用を開始していたところ、平成２６年４月に本格的な運用を開始することが予定されていたものの、同時期になっても一部未完成の部分があり、同年６月の時点でも開発作業が継続していた。

（甲６７、６８）

⑵　Ａによる本件漏えい行為

ア　Ａが本件取得行為を行った際に使用した本件スマートフォンは、Ａｎｄｒｏｉｄ４．１をＯＳとするものであり、ＭＴＰ通信に対応していた。

（前記前提事実⑷ア）

イ　Ａは、平成２５年６月頃、消費者金融等からの債務額が増大し経済的に苦しい状態にあったことから、本件業務で扱う被告ベネッセＣｏの顧客情報を名簿業者に売却して利益を得ることを考えたことがあった。しかし、本件パソコンには、顧客情報を持ち出すことができないように外部記録媒体へのデータ持ち出しを制限するセキュリティがかけられ、ＵＳＢメモリ等の外部記録媒体を接続しても本件パソコンには認識されな

かったことから、顧客情報を持ち出すことは不可能であると考えて諦めていた。

平成２５年７月頃、Ａは、本件スマートフォンを充電するために市販のＵＳＢケーブルを用いて本件スマートフォンを本件パソコンのＵＳＢポートに接続し、充電していたところ、本件パソコンが本件スマートフォンを外部記録媒体として認識し、本件パソコンの画面に、本件スマートフォン内のフォルダ等が表示されたことに気が付いた。Ａは、この状態であれば本件スマートフォンに本件パソコン内のデータを転送して保存することができるかもしれないと考え、本件パソコンに保存されていたファイルを本件スマートフォンに転送してみたところ、当該ファイルを本件スマートフォンに保存することができたため、本件パソコンから顧客情報を記録したファイルを本件スマートフォンに転送できることを認識した。

（甲６５、８８）

ウ　Ａは、平成２５年７月頃から平成２６年６月２７日までにかけて（本件当時）、多摩事務所において、本件データベースから抽出した顧客情報をいったん本件パソコンに保存し、これらの顧客情報を、本件パソコンから、本件パソコンのＵＳＢポートにＵＳＢケーブルを用いて接続した本件スマートフォンへとＭＴＰ通信により転送し、本件スマートフォンの内蔵メモリに保存する等の方法により不正に取得し（本件取得行為）、その後、本件売却行為をした。

（前記前提事実⑷ア、イ）

⑶　Ａｎｄｒｏｉｄスマートフォンの本件当時の利用状況等

ア　スマートフォンやタブレット型端末向けの主なＯＳとしては、Ａｐｐｌｅ　Ｉｎｃ．が提供する「ｉＯＳ」及びＧｏｏｇｌｅが提供する「Ａｎｄｒｏｉｄ」がある。「ｉＯＳ」はＭＴＰ通信に対応していなかったのに対

し、「Ａｎｄｒｏｉｄ」は、タブレット端末については平成２３年5月１０日に発売された「Ａｎｄｒｏｉｄ３．１」から、スマートフォンについては同年１０月１８日に発売された「Ａｎｄｒｏｉｄ４．０」から、それぞれＭＴＰ通信に対応していた。

Ａｎｄｒｏｉｄ４．０以降のＡｎｄｒｏｉｄスマートフォンでは、ＭＴＰが初期設定されていた。

（甲２２、４４、５２、乙４４、弁論の全趣旨）

イ　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Ａｎｄｒｏｉｄスマートフォンには、ＯＳをＡｎｄｒｏｉｄ４．０とするものが多数含まれていた。

また、電気通信事業者各社は、Ａｎｄｒｏｉｄ４．０より前のバージョンのＡｎｄｒｏｉｄをＯＳとするスマートフォンについて、平成２４年夏以降、ＯＳをＡｎｄｒｏｉｄ４．０へバージョンアップするサービスを提供した。

（甲５２、１０５、弁論の全趣旨）

ウ　株式会社MM総研は、平成２５年３月２８日、①同年１月末のスマートフォンの契約数が４０６１万件であり、これをＯＳ別にみると、Ａｎｄｒｏｉｄスマートフォンが２５７０万件（シェアは６３．３％（本項において以下同様。））、iＯＳをＯＳとするスマートフォン（以下「ｉＰｈｏｎｅ」という。）が１４１２万件（３４．８％）、それ以外のＯＳのスマートフォンが７９万件（１．９％）であること、②Ａｎｄｒｏｉｄスマートフォンのシェアは平成２３年３月の４０．４％から２２．９ポイント増加する一方、ｉＰｈｏｎｅのシェアは同月の４９．６％から１４．８ポイント減少していることを指摘している。

また、平成２４年１０月から同年１２月にかけて実施された市場調査において、スマートフォンのＯＳ別販売シェアは、ｉＰｈｏｎｅが６６．２

％、Ａｎｄｒｏｉｄスマートフォンが３１．９％であった旨を指摘する平成２５年１月のインターネット記事や、スマートフォンのＯＳ別シェアは、Ａｎｄｒｏｉｄスマートフォンが平成２４年は２５％、平成２５年は４１．９％、平成２６年は３９．６％であったとするインターネットの記事がある。

（甲４５、乙５０、５１）

エ　日本写真印刷コミュニケーションズ株式会社は、平成２５年８月２日、同社の運営する「スマートフォンＥＣラボ」というウェブサイトにおいて、ＡｎｄｒｏｉｄスマートフォンのＯＳのバージョン別シェアについて、同年４月時点において、契約数のうち半数を超えるものがＡｎｄｒｏｉｄ４．０以降のバージョンのものであったと指摘している。

なお、同シェアについては、日本国内に限定したものではなく世界全体のものを指しているとの指摘がある。

（甲４４、乙６９）

オ　インターネットプライバシー研究所は、被告らから依頼を受けて作成した平成２９年３月１５日付け意見書の中で、①携帯電話端末全体に占めるスマートフォンの割合は、平成２４年３月末時点で２２％、平成２５年３月末時点で３６％、平成２６年３月末で４８％であること、②スマートフォンのうち、ＭＴＰ通信に対応したＡｎｄｒｏｉｄ４．０以降のＯＳを搭載したものの割合は、平成２４年６月時点で０．６９％未満、平成２５年６月時点で１９．８８％、平成２６年６月時点で２１．４１％であること、③したがって、平成２４年から平成２６年において、ＭＴＰ通信に対応したＡｎｄｒｏｉｄ４．０以降のＯＳを搭載したスマートフォンが携帯電話端末全体に占める割合は、平成２４年６月時点で０．１５％未満、平成２５年６月時点で７．１６％、平成２６年６月時点で１０．２８％であることを指摘するほか、④携帯電話端末（スマートフォンと従来型の携帯電話

であるフィーチャーフォンを併せたもの）の契約数が、平成２４年３月末時点で既に１億件を超えており、平成２５年３月末には更に増加し、平成２６年３月には１億２万件を超え、同年１２月末には１億２５１１万件となったことを示す資料を添付している。

（乙４６）

カ　ＭＴＰ対応スマートフォンの登場及び普及等に関する記事のうち、本件当時までに公表され、一般の読者が読むことができたものとしては、次のようなものがあった。

㈠　テクニカルライターのＢは、「モバイルトレンド」と題するウエブ上の連載記事として平成２３年４月２７日に掲載した「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）」と題する記事において、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、これまで使われていたＭＳＣではなく、ＭＴＰを使うものが増えてきたことを指摘し、ＭＴＰには処理があまり高速にならない欠点はあるが、速度の問題は以前に比べると減少してきていること、一方、ＭＴＰにはスマートデバイスとパソコンでのファイル共有に利点があることを解説して、ＭＳＣとＭＴＰの違いを説明し、今後は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した。

㈡　平成２４年１２月２４日発売の雑誌「日経ＰＣ21」２０１３年２月号に掲載された「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」と題する記事には、①スマートフォンとパソコンとの間でファイルをやり取りするには３つの方法があること、１番目の方法は、スマートフォンとパソコンをＵＳＢケーブルで接続する方法であって、この方法が最も確実な方法であること、２番目の方法は、Ｗｉ－Ｆｉ（無線ＬＡＮ）経由で接続する方法であること、３番目の方法は、

インターネット上にファイルを置くクラウドサービスを活用する方法であること、②スマートフォンとパソコンをＵＳＢケーブルで接続してファイルをやり取りする場合の情報通信方式には、ＭＴＰとＭＳＣの二つの方式があり、ＭＴＰの方が簡単であること、③ＡｎｄｒｏｉｄスマートフォンとｉＰｈｏｎｅとではパソコンとの通信方式が異なり、Ａｎｄｒｏｉｄスマートフォンではｍｔｐとｍｓｃの両方の方式が使えることが記載されている。同記事は、平成２５年６月５日、「日経トレンディネット」のウェブサイト上にも掲載されていた。

（甲２１、１１４）

⑷　ＭＳＣとＭＴＰ

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外部記憶装置・媒体（リムーバブルメディア）との間の情報通信方式として用いられているものである。

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であるピクチャー・トランスファー・プロトコル（以下「ＰＴＰ」という。）をベースにして、画像ファイルだけでなく、動画ファイルや音楽ファイル等のその他のファイルの転送も可能にした技術仕様である。

（甲２１、２２、９８、乙４４、６８）

イ　ＭＳＣとＭＴＰの違いは、以下の点にある。

㋐　ＭＳＣとＭＴＰの最大の違いは、ファイルをパソコンで管理するのかあるいはデバイスで管理するのかという点にある。

ＭＳＣ通信では、パソコン側のＯＳでもファイルの管理を行うため、ＯＳを有するデバイス（スマートフォンはこれに含まれる。）との間でＭＳＣ通信を利用する場合には、パソコン側とデバイス側の双方から同一のファイルを対象にした操作を行う可能性があり、パソコン側とデバイス側の双方から同じタイミングで同一のファイルにアクセスしてしまうと操作の重複による不具合が生じるおそれがある。

これに対し、ＭＴＰ通信では、デバイス側のファイルを管理するのはデバイス側のＯＳのみであるため、上記の不具合が生じるおそれがない。

㈠ ＷｉｎｄｏｗｓをＯＳとするパソコンにＭＳＣデバイスを接続すると、パソコンからは、「大容量ストレージデバイス」、すなわち、外付けハードディスクやＵＳＢメモリと同様のものとして認識される。

これに対し、ＷｉｎｄｏｗｓをＯＳとするパソコンにＭＴＰデバイスを接続すると、パソコンからは、「ＷＰＤ」又は「メディアデバイス」として識別される。

（甲２１、２２、９８、１１４、乙４４、６８）

ウ　ＭＴＰは、上記アの開発経緯から、音楽・映像プレーヤーやデジタルカメラ等に採用されていた。スマートフォンについては、ｉＯＳ及びＡｎｄｒｏｉｄ４．０より前のバージョンのＡｎｄｒｏｉｄは、いずれも情報通信方式としてＭＳＣを採用していたが、前記⑶アのとおり、Ａｎｄｒｏｉｄ４．０以降のＡｎｄｒｏｉｄは、ＭＴＰに対応するようになった。

（甲２１、２２、乙６８）

エ　上記イ㈠のとおり、Ｗｉｎｄｏｗｓでは、パソコンに接続されたスマートフォンをスマートフォンとして認識するわけではなく、ＷｉｎｄｏｗｓをＯＳとするパソコンのＵＳＢポートにＵＳＢケーブルを用いてスマートフォンを接続すると、接続したスマートフォンの情報通信方式等によって、「リムーバブルメディア」、「ＷＰＤ」、「イメージングデバイス」、そ

の他の制御対象デバイスとして識別することとなる。したがって、パソコンに搭載されたセキュリティソフトによって、スマートフォンに対する書き出し制御又は接続制御（書き出し制御だけでなく、デバイスからパソコンへのデータの読み込みも制御すること）をしようとする場合には、当該スマートフォンが識別されるデバイスに対する接続制御機能等を有効にする必要があった。

（甲２２、７２、７３）

⑸　本件当時の本件セキュリティソフトの設定

ア　被告ベネッセＣｏ及び被告シンフォームは、被告シンフォームが業務従事者に貸与していた業務用パソコンに株式会社日立ソリューションズのセキュリティソフト「秘文」を搭載していたところ、平成２３年７月、上記業務用パソコンのＯＳをＷｉｎｄｏｗｓ７にバージョンアップした際に、セキュリティソフトも最新の「秘文Ｖｅｒ．９．０」（本件セキュリティソフト）にバージョンアップした。

セキュリティソフト「秘文」には、従前から「リムーバブルメディア、ＣＤ／ＤＶＤ、外付けＨＤＤ」を対象とする接続制御機能が設けられていたが、本件セキュリティソフトにバージョンアップされた際、あらゆるデバイス（〈1〉終端機器であるリムーバブルメディア、外付けＨＤＤ、ＣＤ／ＤＶＤ、その他の制御対象デバイス、ブラックベリー、Ｐａｌｍ、ＯＳ、ウィンドウズモバイル、イメージングデバイス、ＷＰＤ。〈2〉通信機器であるパラレル／シリアルポート、モデム、無線ＬＡＮ、ブルートゥース及び赤外線。）を接続制御することができる機能が付加された。このうち「リムーバブルメディア、ＣＤ／ＤＶＤ、外付けＨＤＤ」については、書き出し制御のみを設定することも可能であり、「リムーバブルメディア」については、ＵＳＢメモリを個体で識別した上での制御が可能であり、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

は暗号化されていた。「リムーバブルメディア、ＣＤ／ＤＶＤ、外付けＨＤＤ」以外のデバイス（ＷＰＤを含む。）については、上記と異なり、接続制御のみが可能であり、書き出し制御のみを設定することはできなかった。

上記バージョンアップの際の本件セキュリティソフトの設定作業は、本件セキュリティソフトの販売代理店であり本件セキュリティソフトの導入運用のサポートを行う会社が行った。その際、被告シンフォームは、特定のＵＳＢメモリ以外の外部記録媒体への書き出しを禁止する方針であった（甲７２、７３）ものの、実際には、「リムーバブルメディア、ＣＤ／ＤＶＤ、外付けＨＤＤ」の書き出し制御機能（ただし、特定のＵＳＢだけは書き出し制御の対象外とするが、当該ＵＳＢに書き出されたデータは暗号化される設定とされた。）のみを有効とする設定がされただけで、ＷＰＤ等の他のデバイスについては、新たに付加された接続制御機能を有効にする設定は行われなかった。

上記販売代理店は、平成２３年８月、被告シンフォームに対し本件セキュリティソフトのパラメーターシートを納品したが、同シートには、「デバイス制御設定」欄の「デバイス使用可否制御を有効にする」、「デバイス個体識別制御を有効にする」、「個体識別ログの出力を有効にする」の３項目のチェック欄のいずれにもチェックが入っておらず、上記３項目については設定がされていないことが示されていた。

被告シンフォームは、上記販売代理店による設定後も、本件セキュリティソフトの設定変更作業を行うことにより、個々のデバイスに対する接続制御機能の設定を変更することが可能であったが、本件セキュリティソフトが導入されてから本件漏えい行為が発覚した平成２６年７月までの間、本件セキュリティソフトの設定を変更したことはなかった。

（甲６７、６８、７１～７３、弁論の全趣旨）

イ　本件セキュリティソフトでは、情報通信方式としてＭＳＣを採用しているスマートフォンは、ＷｉｎｄｏｗｓをＯＳとするパソコンによって「リムーバブルメディア」と識別されるが、本件スマートフォンのようなＭＴＰ対応スマートフォンは、「ＷＰＤ」と識別される。

したがって、本件セキュリティソフトの上記アの設定により、情報通信方式としてＭＳＣを採用している従来型のスマートフォンに対しては、書き出し制御機能が機能していたが、ＭＴＰ対応スマートフォンを含むＷＰＤに対しては、接続制御機能が機能しておらず、パソコンからのデータの書き出しが制御（禁止）されていなかった。

（前記前提事実⑹ア、甲７３、乙７１）

⑹　本件漏えい行為が発覚した後の本件セキュリティソフトの設定

被告シンフォームは、本件漏えい行為が発覚した後である平成２６年７月１４日、本件パソコンから本件スマートフォンへのデータの書き出しが可能であったことにつき、本件セキュリティソフトの販売代理店に問い合わせた上で、自ら、本件セキュリティソフトの設定の見直しを行い、「リムーバブルメディア、ＣＤ／ＤＶＤ、外付けＨＤＤ」については書き出し制御機能の設定を維持するとともに、その他のデバイスについては、赤外線、ブルートゥース、モデム、ＷＰＤ、ウィンドウズモバイル、Ｐａｌｍ ＯＳ、ブラックベリー、その他の制御対象のデバイスにつき、接続制御機能を有効にした。

そして、被告シンフォームは、同月２２日、本件セキュリティソフトのバージョンアップを行い、さらに「イメージングデバイス」についても、接続制御機能を有効にする設定をした。

（甲２５、６７、７１、７３）

⑺　ＭＴＰデバイス制御機能を搭載した商用セキュリティソフトの存在

ア　平成２６年６月時点で、ＭＴＰデバイスに対する何らかの制御機能を搭

載したセキュリティソフトとしては、少なくとも以下の製品があった（㈠は、本件セキュリティソフトである。）。

なお、㈎は、ＭＴＰデバイスに対する書き出し制御機能のみを設定することが可能なものであったが、それ以外は、ＭＴＰデバイスに対し、書き出し制御機能のみの設定をすることができず、接続制御機能（書き出し制御及び読み込み制御の両方を行うもの）の設定しかできないものであった。

㈎　日本電気株式会社の「InfoCage」（対応時期：平成１９年７月）

㈏　株式会社日立ソリューションズの「秘文 AE Information Fortress」（対応時期：平成２１年６月）

㈐　エムオーテックス株式会社の「LanScope Cat」（対応時期：平成２３年３月）

㈑　日本ファインアート株式会社の「TotalSecurityFort」（対応時期：平成２３年８月）

㈒　ハミングヘッズ株式会社の「Evolution/SV」（対応時期：平成２３年１２月）

㈓　株式会社インテリジェントウェイブの「CWAT」（対応時期：平成２４年７月）

㈔　富士通株式会社の「Systemwalker Desktop Keeper」（対応時期：平成２５年８月）

㈕　Ｃ＆Ｃアソシエイツの「発見伝」（対応時期：平成２５年８月）

㈖　クオリティソフト株式会社の「ＱＮＤ Advance」（対応時期：平成２５年９月）

㈗　米国 DeviceLock 社の「DeviceLock」（対応時期：平成２６年２月）

（甲７１、９６、９７、１０１、１０３、乙４７）

イ　上記ア㈎～㈐、㈓、㈔、㈖の各製品の平成２６年６月当時の国内市場におけるシェア（占有率）は、合計４８．９％であったとの報告がある。

（乙４７）

⑻　本件当時までに公表された情報セキュリティに関するガイドライン等

ア　平成９年通産省基準

平成９年通産省基準は、情報システムの機密性、保全性及び可用性を確保することを目的として、自然災害、機器の障害、故意・過失等のリスクを未然に防止し、また、これらが発生したときの影響の最小化及び回復の迅速化を図るため、情報システムの利用者が実施する対策項目を列挙している。

平成９年通産省基準には、その運用基準として、入退館及び入退室に関する「搬出入物」の項目について、その対策項目として、「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。」と記載されており、この対策は、情報システムの重要度の区分に関わらず必要な対策であるとされている。

（甲１４）

イ　平成２１年経産省ガイドライン

㋐　平成２１年経産省ガイドラインは、個人情報保護法８条に基づき同法に定める事項に関して必要な事項を定め、経済産業省が所管する分野及び個人情報保護法３６条１項により経済産業大臣が主務大臣に指定された特定の分野（経済産業分野）における事業者等が行う個人情報の適正な取扱いの確保に関する活動を支援する具体的な指針として定められたものである。

平成２１年経産省ガイドラインは、経済産業大臣が個人情報保護法を執行する際の基準となるものであり、「しなければならない」と記載されている規定については、それに従わなかった場合には、経済産業大臣によって個人情報保護法の規定違反と判断され得る一方、「望ましい」と記載されている規定については、それに従わなかった場合でも、経済

産業大臣によって個人情報保護法の規定違反と判断されることはないものの、個人情報保護法の基本理念を踏まえ、個人情報保護の推進の観点から、できるだけ取り組むことが望まれるとされている。

(イ) 平成２１年経産省ガイドラインは、「安全管理措置（法第２０条関連）」という項目において、①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、組織的、人的、物理的及び技術的な安全管理措置を講じなければならず、その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとし、個人データを記録した媒体の性質に応じた安全管理措置を講じることが望ましいと記載し、②組織的安全管理措置（安全管理について従業者の責任と権限を明確に定め、安全管理に対する規程や手順書（以下「規定等」という。）を整備運用し、その実施状況を確認することをいう。）のうち、個人データの取扱いに関する規程等に記載することが「望まれる」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。）」や、「個人データを利用・加工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、個人データを閲覧だけできる端末では、ＣＤ－Ｒ、ＵＳＢメモリ等の外部記録媒体を接続できないようにする。）」を挙げている。また、③技術的安全管理措置（個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいう。）のうち、「個人データへのアクセス制御」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、「個人デー

タを取り扱う情報システムに導入したアクセス制御機能の有効性の検証（例えば、ウェブアプリケーションのぜい弱性有無の検証）」が挙げられているほか、「個人データを取り扱う情報システムの監視」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、「個人データを取り扱う情報システムの使用状況の定期的な監視」が挙げられている。

㈣　なお、平成２１年経産省ガイドラインは、平成２６年１２月１２日厚生労働省・経済産業省告示第４号により改訂された。同改訂後のガイドライン（以下「平成２６年経産省ガイドライン」という。）では、①組織的安全管理措置に関して、個人データの取扱いに関する規程等に記載することが「望まれる」事項の例示として、「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」及び「個人データを利用・加工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」が記載され、その具体的内容として、「スマートフォン、パソコン等の記録機能を有する機器の接続を制限し、媒体及び機器の更新に対応する」ことが追加された。また、同じく、②物理的安全管理措置（入退館（室）の監理、個人データの盗難の防止等の措置をいう。）に関して、これを実践するために講じることが「望まれる」手法の例示として、「入退館（室）の際における業務上許可を得ていない記録機能を持つ媒体及び機器の持ち込み及び持ち出しの禁止と検査の実施」及び「カメラによる撮影や作業への立ち会い等による記録又はモニタリングの実施」が追加されている。

（甲１３、乙２５～２７）

ウ　ＪＩＳ基準等

ＪＩＳ基準は、事業者に対し、その取り扱う個人情報のリスクに応じて、漏えい、滅失又はき損の防止その他の個人情報の安全管理のために必要かつ適切な措置を講じることを求めている。これを受けて、平成２２年ＪＩ

Ｓガイドラインは、事業者において、個人情報の取得・入力の局面及び利用・加工の局面において講じる対策の例として、個人情報を入力し、又は利用・加工することができる端末に付与する機能を業務上の必要性に基づいて限定することを挙げ、その内容として、個人情報を入力することができる端末や個人情報を閲覧だけすることができる端末では、ＣＤ－ＲＯＭ、ＵＳＢメモリ等の外部記録媒体を接続することができないようにすることを挙げている。

（甲２８）

エ　平成２４年セキュリティガイドライン

一般社団法人日本スマートフォンセキュリティフォーラム（ＪＳＳＥＣ）は、急速に普及しているスマートフォンのセキュリティ上の脅威に対応し、スマートフォンの安全な利活用を図り、その普及を促進するための活動を行うために、関連する様々な分野の企業や団体によって設立された組織である。同法人は、スマートフォンの利用状況に沿った安全利用のためのガイドラインとして策定した平成２４年セキュリティガイドラインにおいて、スマートフォンの特性と留意点に関する項目の中で、スマートフォンのデバイスやＯＳはバージョンアップにより高機能化が進むと考えられ、搭載機能が増えれば利用シーンも増えるとした上で、「ＰＣにＵＳＢケーブルで接続し充電することによる不正な情報流出等も考えられます。」と指摘しており、継続的な対策の検討が求められるとしている。なお、上記ガイドラインが対象とする範囲は、個人所有のスマートフォンを業務利用及び個人利用の兼用で使用する場合も含むとしている。

（甲１１１、乙４４、弁論の全趣旨）

オ　平成２５年ＩＰＡガイドライン

独立行政法人情報処理推進機構（ＩＰＡ）は、経済産業省所管の独立行政法人であり、情報セキュリティ対策を主要事業の一つとしている。

平成２５年ＩＰＡガイドラインは、組織内部者の不正行為による情報漏えい等が度々発生していることに鑑み、企業やその他の組織において必要な内部不正対策の整備を可能とすることを目的としたものであり、違法行為だけでなく、情報セキュリティに関する内部規程違反等の違法とまではいえない不正行為をも内部不正に含めて、組織内における具体的な内部不正対策を検討したものである。平成２５年ＩＰＡガイドラインは、①「個人の情報機器及び記録媒体を業務利用すると、個人の情報機器及び記録媒体の組織による管理が困難であることや、個人と組織の情報が共に扱われることから、ウイルス感染や操作ミス等によって重要情報が漏えいする可能性が高くな」る、「重要情報を取り扱う業務フロア等の領域に個人の情報機器及び記録媒体を持ち込まれると、個人の情報機器や記録媒体に重要情報を格納して持ち出される恐れがあ」るといったリスクの存在を指摘して、「個人のノートＰＣやスマートデバイス等のモバイル機器及び携帯可能なＵＳＢメモリ等の外部記録媒体の業務利用及び持込を制限しなければならない」とし、②その対策のポイントについて、「個人の情報機器及び記録媒体の業務利用及び持込の制限では、その場所で扱う重要情報の重要度及び情報システムの設置場所等を考慮する必要があ」るとした上で、具体的な対策として「重要情報の格納サーバやアクセス管理サーバ等が設置されているサーバルームでは、個人所有のノートＰＣやタブレット端末、スマートフォン等のモバイル機器の持込み・利用を厳しく制限」することや、「個人所有のＵＳＢメモリ等の携帯可能な記録媒体等の持込みを制限」することを定めて運用することが記載されている。

なお、平成２５年ＩＰＡガイドラインについては、平成２６年の前半において、従業員による不正な情報の窃取などの内部者の不正行為によるセキュリティ事故が相次いで報道され、さらに、本件漏えい行為が発生したことから、これらの事例を分析して得られた効果的な対策を反映させる改

訂が行われた。追加された対策のポイントとしては、「重要情報を取り扱う業務フロア等に、個人所有のノートＰＣやタブレット端末、スマートデバイス等のモバイル機器その他の携帯可能な情報機器の持ち込み・利用を厳しく制限する」ことや、「スマートデバイス等のモバイル機器や携帯可能なＵＳＢメモリ等の外部記録媒体の利用を制限するソフトウェアを導入する」こと等が挙げられた。

（甲１５、１６、３６、乙３０、弁論の全趣旨）

カ　平成２５年データセンターガイドブック

日本データセンター協会は、データセンター事業者と、データセンター事業者を取り巻く関連事業者との協力体制を構築し、データセンターへの社会的要請に協力して当たることによって、データセンター事業を強化・発展させることを目的とする特定非営利活動法人である。

平成２５年データセンターガイドブックは、①データセンター（様々な情報通信機器を設置・運用することに特化した建物と設備の総称と、その建物と設備を利用して行われるサービスを意味する。）のエントランス区画において、データセンター事業者から許可された機器や荷物以外をデータセンター内に持ち込ませないことにより、館内、特にサーバに悪影響を与えるおそれのある対象物を排除することを目的として、持込みが制限される品目の一つにＵＳＢメモリ等の情報記録媒体を挙げ、また、②サーバ室からの情報の不正持ち出しの脅威に対する管理策として、画像監視システムの設置を挙げている。

（甲２６、乙２９、弁論の全趣旨）

⑼　本件漏えい行為に関する意見書等

ア　雑誌「日経コンピュータ」の記者であるＣは、平成２６年７月３０日、「ベネッセ事件容疑者はなぜスマホでデータを持ち出せたか、ＩＴ部門は設定の再点検を」と題する記事において、①ＭＴＰの存在が情報漏えい対

策の盲点になり得ること、②Ａｎｄｒｏｉｄスマートフォンの場合、本格的には平成２３年１０月公開のバージョン４．０（Ａｎｄｒｏｉｄ４．０）からＭＴＰによるファイル転送に対応していること、③商用のデバイス制御ソフトでは、一般にＵＳＢマスストレージの使用制限に加え、ＷＰＤ（ファイル転送方式としてＰＴＰやＭＴＰを使用する。）の使用を制限することで、スマートフォンへのデータ転送を制限することができること、④商用のデバイス制御ソフトがＷＰＤの接続制御機能に対応した時期は、株式会社日立ソリューションズ製のものが平成２１年６月、エムオーテックス株式会社製のものが平成２３年３月、日本ファインアート株式会社製のものが平成２３年８月、ハミングヘッズ株式会社製のものが平成２３年１２月、株式会社インテリジェントウェイブ製のものが平成２４年７月、富士通株式会社製のものが平成２５年８月であることを記載するとともに、⑤マイクロソフト製品のセキュリティに詳しいＤ（以下「Ｄ」という。）の発言として、ＭＴＰ通信を制御できていないことが情報漏えい対策の盲点になり得ることは平成２５年頃からセキュリティ技術者の間で話題となっていたこと、また、「Ａｎｄｒｏｉｄ４．０の登場まではＭＴＰ対応端末が少なく、現実的な脅威ではなかった。他企業のＩＴ部門でも、ＵＳＢメモリは制御しても、ＭＴＰの設定まで思い至らない例は多いのでは」とのコメントを紹介している。

（甲２２）

イ　Ｄは、平成２８年２月５日、「情報セキュリティの運用面での脆弱性情報にも届出制が必要なのでないか。」と題する論考をウェブページに掲載した。Ｄは、同論考の中で、スマートフォンを私用で購入して自宅のパソコンに接続させた際の自己の経験から、すでに平成２４年の段階でＡｎｄｒｏｉｄ４．０以降であれば、ファイル転送にＭＴＰが採用されているため、ＵＳＢデバイスの制御による情報漏えい対策では効果がないという脆

弱性が生じており、情報漏えいに悪用できることに気が付いたが、当時は、この問題に気が付いて警鐘を鳴らす個人、国の機関及び組織はなかった旨を記載している。

（乙４８）

ウ　インターネットプライバシー研究所は、被告らから依頼を受けて複数の意見書等を作成しているところ、平成２９年１月２３日付け調査報告書（乙４３）及び平成３０年９月２０日付け意見書（乙６８）の中で、ＭＴＰは、もともとは、デジタルカメラ、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（以下「デジタルカメラ等」という。）をウイ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ものであり、情報セキュリティの現場では、ＭＴＰによる通信を行う機器としては、基本的にデジタルカメラ等が想定されていて、スマートフォンはほとんど念頭に置かれていなかったので、本件当時、ＭＴＰ通信を利用することができるスマートフォンによる情報漏えいのリスクは、情報セキュリティの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ている。

また、インターネットプライバシー研究所は、平成２９年３月１５日付け調査報告書（乙４７）において、平成２６年６月当時販売されていた主要な端末管理・セキュリティ製品について調査を行ったところ、「実用的」なＭＳＣデバイス制御機能は、全ての製品に搭載されていたが、「実用的」なＭＴＰデバイス制御機能は、国内市場シェアが高い端末管理・セキュリティ製品には全く搭載されておらず、「実用的」なＭＴＰデバイス制御機能を搭載していたと認められる製品は、国内市場シェアが微少な１製品にとどまっており、しかも、その製品の初期設定もＭＴＰデバイス制御機能は無効とされていた旨を報告している。なお、同報告書にいう「実用的」とは、少なくとも読み取り専用の設定（書き出し制御のみを行う設定）ができる場合を指し、接続制御しかできないものは「実用的」ではないと扱

っている。

そして、インターネットプライバシー研究所は、平成３０年９月２０日付け意見書（乙６８）において、一般の企業等の業務において、デジタルカメラ、デジタルビデオカメラ、ボイスレコーダーの画像・動画・音声の情報をＭＴＰ通信によりパソコンに取り込むことは日常的に行われているとの認識を示した上で、ＭＴＰ通信による読み取りを制御すれば、ＭＴＰによる通信を行うデジタルカメラ等のデータをＵＳＢ接続によりパソコンに取り込むことが不可能となってしまい、業務上大きな支障が生ずることを指摘している。

（乙３７～４１、４３、４６、４７、６８、６９）

エ　日本ネットワークセキュリティ協会理事等を務めるＥは、被告らから依頼を受けて作成した平成２９年３月３０日付け意見書（乙４４）において、①携帯電話の一種として２０００年代末頃から急速に普及が進んだスマートフォンでは、持ち運びに不便なパソコンと同様の機能が手のひらサイズの機器に搭載され、パソコンとの間で動画や音楽等のマルチメディア・データの共有や連携が容易になったものの、共有される情報は、動画や音楽などマルチメディア・データ程度にとどまり、スマートフォン自体がリムーバブルメディアとして使われることはなく、業務上一般的なテキストやドキュメント等まで扱うリムーバブルメディアとして認識されるまでには至っていなかったこと、②平成２６年当時、ＭＴＰデバイスの想定されていた用途は、パソコンからウィンドウズマルチメディアプレーヤーに動画や音楽などを転送し、同プレーヤーにおいて視聴するなど、私的用途が中心であって、業務用のものではなかったこと（テキストやドキュメント等の情報通信手段としてはＭＳＣが一般的であったこと）、③ＭＴＰ通信によりパソコンの情報をスマートフォンに書き出しても、基本的にはスマートフォン上でそれを閲覧できるわけではなく、さらにスマートフォンから

別のパソコンに情報を移して初めて閲覧できることになるので、パソコンの情報をスマートフォンを使って持ち出しできることには気が付かないことが多いのではないか、そうした情報の持ち出しに気が付くことができるのは、もともと、相当高度な専門的知識を持ち、また、情報の持ち出しの悪意を持っているような場合ではないかと思われるとして、一般的には、ＭＴＰの危険性は認識されていなかったことを指摘している。

なお、上記意見書では、スマートフォンを含む携帯電話を執務室の中に持ち込むことについての本件当時の社会認識について、私物のスマートフォンなどの携帯端末を業務に利用すること（「Bring Your Own Device」以下「ＢＹＯＤ」という。甲１０７・１５頁、１０９・３頁）については、情報保護の観点から一定の管理下に置くとしても、これを促進する方向に傾いており、ＢＹＯＤに係る一定の社会的合意が形成される途上にあったといえるとしている。

（乙４４、４５）

オ　工学院大学名誉教授Ｆは、被告らから依頼を受けて作成した平成３０年１月１５日付け意見書（乙５２）において、平成２６年当時、ＭＴＰを利用した情報漏えいの危険は知られていなかった旨の認識を明らかにしている。

（乙５２）

４　争点⑶（本件漏えい行為について被告シンフォームに過失があるか。）について

⑴　予見可能性について

ア　Ａは、前記前提事実⑷アのとおり、ＵＳＢケーブルを用いて、ＭＴＰ対応の本件スマートフォンを本件パソコンのＵＳＢポートに接続し、ＭＴＰにより本件パソコンから本件スマートフォンに顧客情報のデータを転送する方法によって、本件取得行為をした。

本件取得行為の手段とされたＭＴＰ通信は、前記３認定事実⑷のとおり、従来から多く利用されているＭＳＣ通信とは情報通信方式を異にするものであるから、本件漏えい行為に関して被告シンフォームに原告らの主張する注意義務があるとするには、その前提として、被告シンフォームにおいて、本件当時、パソコンのＵＳＢポートにＵＳＢケーブルを用いてＭＴＰ対応スマートフォンを接続し、ＭＴＰにより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されることを予見し得たことを要するものと解される。

ここでは、便宜上、被告シンフォーム及び被告ベネッセＣｏについて、上記のような予見可能性が認められるかを検討することとする。

イ⑺　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ではなく、通話・通信機能を備えた小型のパソコンであり（甲１０９、１１１、乙４４、弁論の全趣旨）、バージョンアップの都度、高機能化が進むデバイスである。

前記３認定事実⑻のとおり、本件漏えい行為の前から、①平成２１年経産省ガイドラインや平成２５年ＩＰＡガイドライン等は、個人データを入力することができる端末には外部記録媒体を接続することを禁止する方法を推奨し、②平成２５年ＩＰＡガイドラインは、重要情報を取り扱う業務フロア等において、個人の情報機器や外部記録媒体に重要情報を格納して持ち出される危険性があることに鑑み、スマートフォン等のモバイル機器の持込みを制限すべきである旨指摘し、③平成２４年セキュリティガイドラインは、パソコンのＵＳＢポートにスマートフォンを接続して充電することによる不正な情報流出の可能性を指摘していたほか、スマートフォンのデバイスやＯＳはバージョンアップにより高機能化が進み、搭載機能が増えれば利用する機会も増えるため継続的な対策を検討することが求められるとしていたことが認められる。

これらによれば、行政機関その他の団体が、個人情報を取り扱う事業者等に対し、本件当時において、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あることを前提として、情報セキュリティの対策を実施すべきことを指摘していたものと認められる。他にも、本件当時までに、前記３認定事実⑺アのセキュリティソフトの製品に関する情報として、また、情報処理機器を取り扱う企業が集う講習会や情報セキュリティに関する出版物等において、スマートフォンからの情報漏えいの危険性が指摘されていたことも認められる（甲９６、９７、１０１、１０３、１０４、１０６～１１２）。

そして、被告ベネッセＣｏは、被告ベネッセＨＤ及び同社の関係会社（子会社及び関連会社）で構成されるグループ（以下「ベネッセグループ」という。）の中核会社であり、顧客情報を集積して、担当する教育事業及び生活事業の活動に利用しており、また、被告シンフォームは、ベネッセグループの情報処理全般を支えるＩＴ機能会社であり、グループ各社が手掛ける事業の要望や目的に合わせたシステムの構築を担っていたもので、被告ベネッセＣｏの上記各事業の活動を支える大規模な顧客管理システムの保守・管理・運用の業務を担当していた（前記前提事実⑴及び⑵ア、甲４６、７９）。これらの事実に照らせば、被告ベネッセＣｏ及び被告シンフォームにおいては、その事業を展開する上で集積される個人情報が重要資源となる以上、効率的な事業展開のためのデータベース化やシステム化を進めるに際しても、細心の情報セキュリティ対策を講じる必要があることは十分認識されていたことが推認される。

以上によれば、被告ベネッセＣｏ及び被告シンフォームにおいては、本件当時、公表されていた情報をもとにスマートフォン等のモバイル機器を利用した情報漏えいがあり得ることを十分想定することができたといえる。

さらに、①前記３認定事実⑸アのとおり、平成２３年７月にセキュリティソフトを本件セキュリティソフトにバージョンアップした際、被告シンフォームは、特定のＵＳＢメモリ以外の外部記録媒体への書き出しを禁止するという方針を採っていたこと、②本件当時、被告シンフォームの顧客分析課課長であったＧ（以下「Ｇ」という。）は、被告ベネッセＣｏのＩＴ戦略部に出向した経歴を有する者であるところ、被告ベネッセＣｏによる被告シンフォームに対する監査の際、私物スマートフォンの執務室への持ち込みや業務用パソコンへの接続を禁止していないことが問題にされなかった理由について、被告シンフォームにおいて導入していた本件セキュリティソフトによって書き出し制御がされていることを挙げているから（甲６８）、これは本件業務に関与する者が私物スマートフォンを利用して情報を漏えいさせることがあり得るとの認識を前提とするものであると認められることからすると、被告ベネッセＣｏ及び被告シンフォームは、本件当時、スマートフォンを含む外部記録媒体一般について、これらを業務用パソコンのＵＳＢポートに接続する等の方法により顧客情報を不正に取得される危険があることを認識していたことが認められる。

⑷　前記３認定事実⑶のとおり、①平成２３年１０月に初めてＭＴＰに対応したＡｎｄｒｏｉｄ４．０をＯＳとするＡｎｄｒｏｉｄスマートフォンが発売され、平成２４年夏に発売されたＡｎｄｒｏｉｄスマートフォンはＡｎｄｒｏｉｄ４．０をＯＳとするものが多数を占め、その結果、平成２５年には、ＭＴＰに対応しているＡｎｄｒｏｉｄ４．０をＯＳとするＡｎｄｒｏｉｄスマートフォンが国内において少なくとも数百万台を超えて販売されていたといえることのほか、②電気通信事業者各社が旧バージョンのＡｎｄｒｏｉｄのＯＳについてＡｎｄｒｏｉｄ４．０へバージョンアップするサービスを提供していたことから、既存のＡｎｄ

ｒｏｉｄスマートフォンのうち相当の台数について、Ａｎｄｒｏｉｄ４．０へのバージョンアップが行われたことが推認される。また、前記３認定事実⑶カによれば、遅くとも本件当時までには、Ａｎｄｒｏｉｄスマートフォンのうち新しく発売されていた機種について、パソコンとの間の情報通信方式として新たにＭＴＰを採用していることは、一般に知り得るところであったことが認められる。

そうすると、前記前提事実⑹ウのとおり、多摩事務所では、私物スマートフォンを執務室内に持ち込むことや業務用パソコンに接続して充電することが許容されていたのであるから、被告ベネッセＣｏ及び被告シンフォームは、本件当時、ＭＴＰ対応スマートフォンが被告シンフォームの執務室内で業務用パソコンに接続される可能性を認識することができたというべきである。

⑺ウ　そして、ＭＴＰが、前記３認定事実⑷ア及びウのとおり、デジタルカメラの画像転送プロトコル（ＰＴＰ）をベースにして、画像ファイルだけでなく、音楽・動画ファイル等のその他のファイルの転送も可能にした規格であり、バージョンアップにより年々高機能化の進むスマートフォンの情報通信方式として、ＭＳＣに代替する技術仕様として採用されていること（前記３認定事実⑶カ及び⑷ウ）からすると、ＭＴＰ対応スマートフォンも、転送できるファイルの範囲はＭＳＣによる情報通信方式を採用している従来型のスマートフォンと基本的に変わりはないことが推認されるため（前記３認定事実⑶カ。このことを否定する的確な証拠は見当たらない。）、被告ベネッセＣｏ及び被告シンフォームにおいて、ＭＴＰ対応スマートフォンにより、ドキュメントファイルを転送することができることを認識することは可能であったというべきである。

⑺エ　以上によれば、被告ベネッセＣｏ及び被告シンフォームは、本件当時、本件データベースにアクセスする権限を有する者において、業務用パソ

コンのＵＳＢポートにＵＳＢケーブルを用いてＭＴＰ対応スマートフォンを接続し、ＭＴＰにより業務用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、顧客情報を不正に取得し得ることを予見することができたと認めることができる。

ウ㋐　これに対し、①本件取得行為の前にはＭＴＰ対応スマートフォンへの不正な情報書き出しの事例が存在したとの報告は見当たらないこと、②前記３認定事実⑼のとおり、ＭＴＰ通信を利用した不正な情報書き出しの危険性について、平成２４年には既に認識していたとする者や、平成２５年頃からセキュリティ技術者の間で話題となっていたとする指摘はあるものの、これらは当時公表されておらず、他方、専門家の中には、上記危険性を認識していた者はいなかったと指摘する者もいること、③前記３認定事実⑻に加え、証拠（乙４４）及び弁論の全趣旨によれば、本件当時までに、情報書き出しの危険性についてＭＴＰ対応スマートフォンに関する危険性であることを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いことが認められる。

また、前記３認定事実⑼ウのとおり、インターネットプライバシー研究所は、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デバイス制御機能は、国内市場シェアが高い製品には全く搭載されておらず、「実用的」なＭＴＰデバイス制御機能を搭載していたと認められる製品は、国内市場シェアが微少な１製品にとどまっており、しかも、その製品の初期設定ではＭＴＰデバイス制御機能は無効とされている旨を報告している。

㋑　しかしながら、本件当時までに、インターネット上の記事において、企業を対象とするスマートデバイスに関する講演会等において、ＭＴＰ通信に対応したＡｎｄｒｏｉｄスマートフォンを利用した情報漏えいの危険性について指摘されていたことが認められ（甲１０４、１０６、１

０７）、このことと本件当時におけるＭＴＰ通信に対応したＡｎｄｒｏｉｄスマートフォンの国内の普及状況（前記３認定事実(3)）を併せて考えると、被告ベネッセＣｏ及び被告シンフォームは、新たに登場したＭＴＰ対応スマートフォンに対する情報漏えい対策の必要性を認識し得たというべきである。この点は、本件当時までにＭＴＰ対応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がなかったことによって左右されるものではない。

なお、被告らは、被告ベネッセＣｏ及び被告シンフォームはデバイスやセキュリティソフトの研究者でもなければ開発事業者でもなく、それらの一般ユーザーでしかないのであって、情報セキュリティに精通しているわけではないと主張する。情報セキュリティについては各企業の業務、環境及びリスク等を勘案して必要な対策が求められる（乙１５）ところ、被告ベネッセＣｏ及び被告シンフォームが事業活動上取り扱う対象は顧客からの大量の個人情報であるから、情報管理に関する社会一般の認識に照らしても被告ベネッセＣｏ及び被告シンフォームは情報セキュリティ対策に細心の注意を払うべき立場にあり、実際にもそうした意識の下で企業活動を遂行しているものと推認される。そうであれば、被告ベネッセＣｏ及び被告シンフォームは、情報セキュリティ対策において、その内容に精通しているか否かにかかわらず被告ベネッセＣｏ及び被告シンフォームの事業活動の性質から必要とされる対策を講じなければならない立場にあり、実際にそのための対策を講じてきたといえるから、被告らの上記主張は被告ベネッセＣｏ及び被告シンフォームの予見可能性の有無に影響を及ぼすものではない。

また、前記３認定事実(7)によれば、ＭＴＰデバイスに対して接続制御機能を有する商用セキュリティソフトは、平成１９年から販売が開始さ

れており、平成２５年８月時点では少なくとも８社からの製品が販売されていたのであって、平成２６年６月時点では広く利用されるに至っていたことが認められることからすれば、被告ベネッセＣｏ及び被告シンフォームにおいて、ＭＴＰデバイスに対する情報漏えい対策が必要であることを認識できたはずであることには変わりがない。

インターネットプライバシー研究所は、同研究所が作成する意見書において、平成２６年６月当時、「実用的」なＭＴＰデバイス制御機能を搭載していたセキュリティソフトは国内市場シェアが微小な１製品のみであったと述べるが（前記３認定事実⑼ウ）、これは、インターネットプライバシー研究所が、ＭＴＰデバイスに対して読み取り専用の設定（書き出し制御のみを行う設定）ができるセキュリティソフトのみを「実用的」であるとし、接続制御しかできないセキュリティソフトは「実用的」でないとする独自の評価をしていることによるものである。パソコンに保存されている情報を管理し、当該パソコンを通じて情報を管理する場面において、リムーバブルメディア等からパソコンに情報を転送する場合を、その逆方向である情報の転送の場合より保護する必要が高いとすることに合理的理由は見い出せず、接続制御のみ可能なものを実用的でないと評価することに合理性があるとはいえないから、上記記載は、被告ベネッセＣｏ及び被告シンフォームの予見可能性についての上記認定を左右するものではない。

以上によれば、前記㋐の各事情は、被告ベネッセＣｏ及び被告シンフォームに予見可能性があったとする前記イの認定を覆すに足りるものとはいえず、他にこの認定を左右するに足りる的確な証拠は見当たらない。

⑵　私物スマートフォン等の持込禁止措置義務違反について

原告らは、被告シンフォームには、本件当時、業務委託先を含めた従業員による私物スマートフォン等の執務室への持込みを禁止する措置を講ずるべ

き注意義務（持込禁止措置義務）があったと主張する。

確かに、情報セキュリティについては、組織の外部からの脅威のみならず、組織内部の脅威（情報漏えい、情報持ち出し及び不正操作等）についても対策が必要であるから（乙１５等）、記録媒体となり得る私物スマートフォンを執務室に持ち込むことを禁止すれば、情報漏えいを防ぐ可能性が高まるものといえ、平成２５年ＩＰＡガイドライン、平成２５年データセンターガイドブックにも、記録媒体となり得る私物スマートフォン等の業務フロア等への持込みを制限することが望ましい等の記載がある（前記３認定事実⑻オ及びカ）。また、私物スマートフォンの執務室内への持込みを禁止すること自体は、比較的容易に取り得る措置といえる。

しかしながら、重要情報を格納するサーバ等が設置されているサーバルームであればともかく、個人情報や機密性の高い情報を扱う業務以外の他の業務も行う執務室においてまで、私物スマートフォンの持込みを一切禁止することは、当該執務室で労務に従事する者に対して大きな制約となるし、執務室の入退室を管理する負担が増大することにもなる。また、一定のリスクを認識した上で個人所有のスマートフォンを企業内に持ち込んで業務に活用すること（ＢＹＯＤ）については、費用削減や業務効率化等といったメリットが企業側に生じることもあると認められ（甲１０７）、後記⑷のとおり、個人情報の不正取得を防止する他の効果的な代替手段も存在することが認められる。

以上によれば、本件当時、被告シンフォームが私物スマートフォンの持込禁止措置をとることは情報漏えい防止に効果的であったということはできるものの、これを行わなければならない注意義務が生じていたとまでいうことはできない。

⑶　業務用パソコンに対するＵＳＢ接続禁止措置義務違反について

原告らは、被告シンフォームには、本件当時、業務用パソコンのＵＳＢポ

ートを物理的にふさいだり、業務用パソコンのＵＳＢポートに私物スマートフォンを接続することを禁止するルールを設けたりするなどして、業務用パソコンのＵＳＢポートに私物スマートフォンを接続することを禁止する措置を講ずるべき注意義務（ＵＳＢ接続禁止措置義務）があったと主張する。

確かに、業務用パソコンのＵＳＢポートへ私物スマートフォンを接続することを禁止すれば、業務用パソコンからの情報漏えいを防止できる可能性が高まるものといえ、①平成２１年経産省ガイドラインは、個人データを入力できる端末にＵＳＢメモリ等の外部記録媒体を接続することができないようにすることが望ましいとし（前記３認定事実⑻イ㈠）、②平成２２年ＪＩＳガイドラインは、業務上の必要性に基づく対策として、個人情報を入力・閲覧する端末にはＵＳＢメモリ等の外部記録媒体を接続することができないようにすることを挙げており（前記３認定事実⑻ウ）、③平成２５年ＩＰＡガイドラインは、具体的な内部不正対策として個人のノートパソコンやスマートフォン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を制限することを挙げている（前記３認定事実⑻オ）。

しかしながら、パソコンのＵＳＢポートは、外部記録媒体を接続するために使用されるのみならず、マウス、キーボード、プリンタ等の業務上必要な装置を接続する用途としても使用されるのであるから、全てのＵＳＢポートを物理的にふさぐことになれば業務上著しい支障を生じることになる上、接続を禁止するルールを設けたとしても、故意に不正行為を試みる内部者に対しては実効性のある情報漏えい対策となるとは考え難い。また、後記⑷のとおり、個人情報の不正取得を防止する他の効果的な代替手段も存在することが認められる。

以上によれば、本件当時、被告シンフォームがＵＳＢ接続禁止措置をとることの有効性には疑問があり、その弊害も大きいことを考慮すれば、ＵＳＢ接続禁止措置をとる義務があったということはできない。

⑷　情報書き出し制御措置義務違反について

ア　原告らは、被告シンフォームには、本件当時、ＭＴＰ通信に対する書き出し制御機能又は接続制御機能を備えたセキュリティソフトを業務用パソコンに搭載することにより、ＭＴＰによる業務用パソコンからデバイスへの情報の書き出しを制御する措置を講ずるべき注意義務（情報書き出し制御措置義務）があったと主張する。

イ　前記３認定事実⑸のとおり、被告シンフォームにおいては、本件当時、本件セキュリティソフトの設定を変更して、ＷＰＤについて接続を制御する設定にすれば、業務用パソコンからＭＴＰ対応スマートフォンへのデータの書き出しを防止することが可能であり、かつ、これがＭＴＰ対応スマートフォンを利用した情報漏えいを防止する最も効果的な方法であったといえる。

そして、前記３認定事実⑹のとおり、被告シンフォームが、本件漏えい行為の発覚後、本件パソコンから本件スマートフォンへのデータの書き出しが可能な状態であったことを認識し、本件セキュリティソフトの設定の見直しを行い、ＷＰＤについて接続制御機能を有効にする設定に変更したこと（その後、この設定がさらに変更されたことを認めるに足りる証拠は見当たらない。）からすれば、上記の設定を変更するまでの間においても、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業務上の必要性は特段なかったことが認められるから、被告シンフォームにおいて、本件セキュリティソフトによるＷＰＤに対する接続制御を有効にすることは可能であったといえる。

ウ　パソコン及びこれに接続される各種デバイスは、バージョンアップにより高機能化が進むのであり（前記⑴イ㋐）、その技術進歩のスピードは速い。本件取得行為は、①被告シンフォームの業務用パソコンのＯＳがＭＴＰに対応しているＷｉｎｄｏｗｓ７となり、かつ、②本件スマートフォン

がＭＴＰ対応スマートフォンであったことから、可能となったものであり、パソコン及びスマートフォンのそれぞれについて技術が進展したことにより新たな脆弱性が発生したことによるものといえる（乙４４）。

被告シンフォームは、平成２３年７月に行われたセキュリティソフトのバージョンアップによって本件セキュリティソフトを導入したものであるが、販売代理店の説明又は本件セキュリティソフトの取扱説明書やパンフレットの閲読等により（前記３認定事実⑸ア）、①本件セキュリティソフトは、あらゆるデバイスに対して接続制御が可能であること、②被告シンフォームにおいて接続制御をする必要があると考えるものがＷｉｎｄｏｗｓをＯＳとするパソコンにおいてどのようなデバイスとして識別されるのかを考慮して、それぞれについて接続制御機能を有効にするか無効にするかの設定を決める必要があることを認識し得たことが認められる。

そして、被告シンフォームは、ベネッセグループの情報処理全般を支えるＩＴ機能会社として、グループの中核企業である被告ベネッセＣｏの顧客管理システムの保守・管理・運用の業務を担当していたものであり（前記⑴イ㋐）、スマートフォンによる情報漏えいの危険性を認識していながら（前記⑴イ）、私物スマートフォンの執務室への持込みや業務用パソコンに接続して充電することを許容する一方、本件データベースと業務用パソコンとの間の通信量はアラートシステムの対象とせず（前記前提事実⑹イ及びウ）、本件データベースに対する情報漏えい防止を本件セキュリティソフトに依存していたのである（甲６８）から、本件セキュリティソフトの取扱説明書の閲読又は販売代理店への照会等によって、スマートフォンの情報通信方式の追加・変更に対応して本件セキュリティの設定を変更する必要がないかを確認し、適切な対応をしなければならない立場にあったというべきである。技術の進歩に伴い新たに生じた脆弱性を認識し対応策を講じるには一定の期間を要するとしても、平成２３年１０月にＡｎｄ

ｒｏｉｄ４．０をＯＳとするＭＴＰ対応スマートフォンが発売された後、本件取得行為が最初に行われた平成２５年７月頃までには約１年半以上が経過しており、この間にＭＴＰ対応スマートフォンの普及が進み、ＭＴＰ対応スマートフォンとパソコンとの連携に関する記事が一般読者向けの雑誌に掲載されるようにもなっていたこと（前記３認定事実⑶）を考慮すると、被告シンフォームには、遅くとも平成２５年７月頃までには、本件セキュリティの設定を見直し、これを適切な設定に変更すべき注意義務があったものといえる。この点は、平成２３年７月時点において本件セキュリティソフトの設定作業に関する事務を担当したのが本件セキュリティソフトの販売代理店であったとしても（前記３認定事実⑸ア）、その結論が左右されるものではない。

エ　それにもかかわらず、被告シンフォームは、平成２３年７月頃から本件当時まで本件セキュリティソフトの設定の見直しを行っておらず、その結果として、業務用パソコンからＭＴＰ対応スマートフォンへのデータの転送を可能としていたのであるから、被告シンフォームには、本件当時、情報書き出し制御措置義務に違反した過失があったというべきである。

オ　この点について、被告シンフォームは、本件当時、ＭＴＰ対応スマートフォンに対する書き出し制御措置を講じることは経済産業省のガイドラインその他のガイドライン等に記載されておらず、また、被告シンフォームは一般的水準に照らして明らかに高度な情報セキュリティ対策を講じていたものであるから、被告シンフォームに情報書き出し制御措置義務があるとするのは過大な義務を負担させるものである等と主張する。

しかしながら、被告シンフォームは、既に検討したように、ベネッセグループの情報処理全般を支えるＩＴ機能会社であり、大量の顧客に関する情報を取り扱う本件システムにおける本件業務の委託を受ける立場

にあり、本件当時、ＭＴＰ対応スマートフォンによる情報漏えいの危険性を予見し、これを回避するための接続制御機能を有効にする措置を講じることができたのであり、本件セキュリティソフトの導入後であっても接続制御に関する設定を変更することは可能であったから（前記３認定事実⑸ア）、ガイドライン等に記載がなかったことをもって、前記の認定判断が左右されるものではないし、被告シンフォームが講じてきたとする他の情報セキュリティ対策が存在することをもってしても、注意義務の存否に関する認定判断が左右されるものではない。この点に関する被告シンフォームの主張は採用することができない。

⑸　小括

以上によれば、被告シンフォームには、本件漏えい行為について、情報書き出し制御措置義務違反の過失があったことが認められる。

５　争点⑷（本件漏えい行為について被告ベネッセＣｏに過失があるか。）について

⑴　予見可能性について

本件漏えい行為に関して被告ベネッセＣｏに原告らの主張する注意義務があるとするには、その前提として、被告ベネッセＣｏにおいて、本件当時、パソコンのＵＳＢポートにＵＳＢケーブルを用いてＭＴＰ対応スマートフォンを接続し、ＭＴＰによりデータを転送する方法によって個人情報を不正に取得されることを予見し得えたことを要すると解されるところ、被告ベネッセＣｏについて上記予見可能性が認められることは、前記４⑴イで説示したとおりである。

この点について、被告ベネッセＣｏは、専門性・信頼性の高い委託先に委託したにすぎないとして、予見可能性は認められないと主張する。

しかしながら、前記４⑴で検討したように、被告ベネッセＣｏ及び被告シンフォームの予見可能性は、スマートフォンが通話・通信機能を備えた小型

のパソコンであって年々バージョンアップにより高機能化が進むデバイスであり、スマートフォンを利用した情報漏えいの危険性が指摘される中で、実際にＭＴＰ対応スマートフォンの普及率が高まるとともに、平成１９年以降ＭＴＰデバイスに対する接続制御機能を有する商用セキュリティソフトが販売され、平成２５年８月頃には多数の販売事業者から販売されている状況にあったことに加え、顧客から個人情報を集積して事業活動に利用していた被告ベネッセＣｏが、リスク管理と効率化を図るために、ＩＴ機能会社である被告シンフォームに対して本件システムに係る本件業務を委託していたことから認められるものである。そして、被告ベネッセＣｏは、大量の顧客情報を集積してこれを事業活動に利用していたことから、情報セキュリティ対策に細心の関心を持つべき立場にあり、実際にそうした前提で企業活動を遂行していたものと推認されるのであるから、本件システムに係る本件業務を委託していたか否かという点と同社の予見可能性が関連するものとはいえない。また、上記の予見可能性の内容は、情報セキュリティに関する専門業者でなければ予見できない内容であるとは認められず、被告ベネッセＣｏが、委託先の被告シンフォームにおいて個人情報を保護するための様々なセキュリティ対策を講じていることを信頼していたとしても、その予見可能性が否定されるものではない。この点に関する被告ベネッセＣｏの主張は採用することができない。

⑵　委託先の選定及び監督に関する注意義務違反について

ア　原告らは、被告ベネッセＣｏは、個人情報保護法２２条等からすれば、本件当時、本件業務の委託先を選定するに当たり、適切に個人情報を管理する体制にある業者を選定するべき注意義務及び委託先において個人情報保護法２０条に基づく安全管理措置が適切にとられているかを監督するべき注意義務（委託先選定監督義務）を負っていたにもかかわらず、これを怠ったと主張する。

イ(ア)　被告ベネッセＣｏは個人情報取扱事業者（個人情報保護法２条３項）に該当するものであるところ、同法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。」と規定する。

そして、平成２１年経産省ガイドラインは、「委託先の監督（法第２２条関連）」の項目について、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、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よう、委託を受けた者に対し必要かつ適切な監督をしなければならないとし、その際には、取扱いを委託する個人のデータの内容を踏まえ、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じた必要かつ適切な措置を講じるものとするとして「必要かつ適切な監督」に関して、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としており、このうち、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については、委託契約で盛り込んだ内容の実施の程度を相互に確認することが望ましいとしている。そして、個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項として、「個人データの取扱状況に関する委託元への報告の内容及び頻度」や「契約内容が遵守されていることの確認（例えば、情報セキュリティ監査なども含まれる。）」が挙げられている（甲１３、乙２５）。

また、ＪＩＳ基準は、「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。」等を例示する（甲２８）。

(イ) ところで、被告ベネッセＣｏは、〈１〉校外学習事業として、幼児から高校生を対象とした通信教育講座「進研ゼミ」、「こどもちゃれんじ」を中心に学習塾・予備校の事業を行うほか、〈２〉大学入試模擬試験等の学校向け教育事業を展開するのに加え、〈３〉妊娠・出産・育児雑誌や生活情報誌等の通信販売事業等による生活関連事業も展開していたもので（甲３、弁論の全趣旨）、こうした事業展開に伴って顧客の個人情報が大量に被告ベネッセＣｏに集積されていたと認められるところ、個人情報が顧客等から提供される前提として、原告らを含む被告ベネッセＣｏの顧客等は、被告ベネッセＣｏが上記(ア)のガイドライン等に従って個人情報保護法２２条所定の義務を果たすことを信頼しているからこそ、被告ベネッセＣｏに対して個人情報を提供してきたものと認められる。そして、被告ベネッセＣｏは、このようにして提供された顧客情報を大量に集積し、これらを事業活動に活用し、顧客等の年齢に適したマーケティングを行うなどして利益を上げてきたことが認められる（前記前提事実(2)ア、甲６７、７０）。そうすると、個人情報取扱事業者としての被告ベネッセＣｏにおいて遵守することが求められる上記(ア)のガイドラインの内容等も踏まえると、被告ベネッセＣｏには、本件システムの開

発等のために大量の顧客情報の取扱いを被告シンフォームに委託するに当たり、原告らを含む顧客等に対しても、信義則上、委託先選定監督義務を負っていたというべきである。

ウ　前記⑴のとおり、被告ベネッセＣｏは、本件当時、本件データベースにアクセスする権限を有する者において、業務用パソコンのＵＳＢポートにＵＳＢケーブルを用いてＭＴＰ対応スマートフォンを接続し、ＭＴＰにより業務用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、顧客情報を不正に取得し得ることを予見し得たことが認められる。

そして、被告シンフォームには、本件漏えい行為につき、情報書き出し制御措置義務違反が認められるところ（前記４⑷）、被告ベネッセＣｏが被告シンフォームに対して本件セキュリティソフトの設定が適切に行われているかどうかについて適切に報告を求めていれば、被告シンフォームにおいて、ＭＴＰ対応スマートフォンに対する書き出し制御又は接続制御が不十分であることに気が付き、自ら本件セキュリティソフトの設定変更等を行い、あるいは、被告ベネッセＣｏにおいて、ＭＴＰ対応スマートフォンに対する書き出し制御又は接続制御が不十分であることを把握し、被告シンフォームに対して本件セキュリティソフトの設定変更等を指示することができたというべきである。

しかしながら、被告ベネッセＣｏは、被告シンフォームに対して本件業務を委託した後、被告シンフォームに対する定期的な委託先監査を行っていたものの、被告シンフォームが採用していた本件セキュリティソフトの設定内容については、委託先監査の対象項目としていなかったことが認められる（甲２５、６９、乙４３）。本件セキュリティソフトによる書き出し制御又は接続制御は、被告シンフォームにおける重要な情報漏えい防止策であったこと（前記４⑷ウ）を考慮すると、被告ベネッセＣｏによる被告シンフォームに対する委託先監査は不十分であったといわざるを得ない。

⑶　小括

以上によれば、被告ベネッセＣｏには、本件漏えい行為について、業務委託先である被告シンフォームに対する監督を怠った過失があったと認めることができる。

他方、被告ベネッセＣｏが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、適正な選定基準に反していたことなど被告ベネッセＣｏの注意義務違反を基礎付ける事実を認めるに足りる的確な証拠は見当たらないから、委託先の選定に関する被告ベネッセＣｏの注意義務違反についての原告らの主張は理由がない。

６　争点⑸（被告ベネッセＣｏ及び被告シンフォームの行為に違法性が認められるか。）について

前記２で漏えいの事実を認定した個人情報について、原告らにおいて、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、上記個人情報は、原告らのプライバシーに係る情報として法的保護の対象となるものであり、本件漏えい行為によって、原告らは、そのプライバシーを違法に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・判例タイムズ１４４２号４６頁参照）。そうすると、前記４及び５で認定した本件漏えい行為に係る被告シンフォーム及び被告ベネッセＣｏの過失行為により、原告らは、そのプライバシーを違法に侵害されたというべきである。

この点、被告シンフォーム及び被告ベネッセＣｏは、被告シンフォーム及び被告ベネッセＣｏの本件漏えい行為に係る行為は、社会通念上許容される限度を逸脱し、違法性を帯びる行為であるとはいえないと主張する。しかしながら、上記４及び５で認定した被告シンフォーム及び被告ベネッセＣｏの過失行為の内容に加え、本件の顧客情報は、Ａによって名簿業者３社に対して売却された

上、さらに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るから（前記前提事実⑷イ及びエ）、もはやその回収は困難であることなどを考慮すると、被告シンフォーム及び被告ベネッセＣｏの本件漏えい行為に係る過失行為が原告らの受忍限度の範囲内にとどまるということはできない。損害の有無及び程度の検討において被告シンフォーム及び被告ベネッセＣｏ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、被告シンフォーム及び被告ベネッセＣｏの過失行為が、社会通念上許容される限度にとどまり、違法性を欠くとはいえない。

被告シンフォーム及び被告ベネッセＣｏは、個人情報漏えい事故の被害者とされる者が、個人情報の管理について個人情報取扱事業者に対して寄せる合理的期待は、いかなることがあろうとも絶対に個人情報漏えい事故を発生させないというものではなく、個人情報が法令に則って取り扱われ、社会的に相応の管理措置がとられることであり、万一漏えいがあった場合は、事案に応じた調査、再発防止あるいは適宜の措置がとられることであるとして、被告シンフォーム及び被告ベネッセＣｏはそうした合理的期待を裏切ったわけではないので、被告シンフォーム及び被告ベネッセＣｏの行為は、社会通念上許容される限度を逸脱した違法な行為ではない旨の主張をする。

この点につき、本件漏えい行為に係る被告シンフォーム及び被告ベネッセＣｏの過失行為により、原告らのプライバシーが侵害されたことは上記で検討したとおりである。加えて、本件記録を検討しても、原告らが被告シンフォーム及び被告ベネッセＣｏに対して寄せていた期待が被告シンフォーム及び被告ベネッセＣｏの主張する範囲にとどまるものであったことを認めるに足りる的確な証拠は見当たらない。この点に関する被告ベネッセＣｏ及び被告シンフォームの主張は採用することができない。

7　争点⑹（被告ベネッセＣｏは、被告シンフォームの不法行為について使用者責任を負うか。）について

⑴　被告シンフォームの不法行為について

前記４及び６のとおり、被告シンフォームには、本件漏えい行為について、情報書き出し制御措置義務に違反した過失があり、これによって原告らのプライバシーが違法に侵害されたものであるから、被告シンフォームは原告らに対して不法行為責任を負う。

⑵　使用者性

被告ベネッセＣｏが、被告シンフォームとの関係で、民法７１５条１項本文の「ある事業のために他人を使用する者」といえるためには、被告ベネッセＣｏが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認められることが必要である。

しかしながら、被告ベネッセＣｏと被告シンフォームは法人格を別にするものであって、被告ベネッセＣｏが、別法人である被告シンフォームの個々の業務についてまで当然に指揮監督権を有するということはできない。

そして、被告ベネッセＣｏと被告シンフォームは、本件業務に関して業務委託基本契約を締結し（甲４２）、被告シンフォームは自社の業務として本件業務を行っていたこと、Ａが被告ベネッセＣｏから直接業務等を指示されていた形跡がないこと（乙２～１２）も踏まえると、被告ベネッセＣｏが、上記契約上の業務委託の範囲を超えて、別法人である被告シンフォームに対して、日常の業務を個別具体的に指示するなど、実質的な指揮監督をしていたとはいえず、他にこれを認めるに足りる的確な証拠は見当たらない。

この点について、原告らは、被告ベネッセＣｏが被告シンフォームに対して研修等を指示していたことや月次報告会を開催して委託業務の進捗を確認していたこと等の事実は、被告ベネッセＣｏの被告シンフォームに対する使用者性を基礎付ける事実である旨主張する。

しかしながら、被告ベネッセＣｏは、被告シンフォームに対して、本件業務委託契約を締結して本件業務を委託していたのであるから、契約上の委託

者として、委託業務の一般的な説明を行うことや、委託業務の進捗を確認することは契約上当然に予定されているところであり、これらのことをもって直ちに民法７１５条の規定にいう使用者に当たることを基礎付けるものとは認め難い。

また、被告ベネッセＣｏの従業員が、被告シンフォームに出向し、被告シンフォームの従業員の立場で被告ベネッセＣｏから受託していた業務に従事していた期間があるとしても、ベネッセグループに属する企業間で従業員を出向させる関係が存在したというにとどまり、これをもって、直ちに、被告ベネッセＣｏと被告シンフォームとの間に使用者と被用者と同視できるような実質的指揮監督関係が存在したということはできない。

この点に関する原告らの主張は採用することができない。

⑶　小括

以上によれば、被告ベネッセＣｏが、原告らに対し、本件漏えい行為につき、被告シンフォームを被用者とする使用者責任を負う旨の原告らの主張は、その余の点について判断するまでもなく、採用することができない。

８　争点⑺（被告シンフォームは、Ａの不法行為について使用者責任を負うか。）について

⑴　Ａの不法行為について

前記前提事実⑷ア～ウのとおり、Ａは、被告ベネッセＣｏの保有する顧客情報（原告らが被告ベネッセＣｏに提供した本件の個人情報を含む。）を不正に取得し（本件取得行為）、これを名簿業者に販売すること（本件売却行為）によって、前記６のとおり、原告らのプライバシーを侵害したのであるから、原告らに対して不法行為責任を負う。

⑵　使用者性について

ア　前記３認定事実⑴のとおり、Ａは、被告シンフォームにおいて、本件業務を所管する顧客分析課内のグループに属し、多摩事務所の執務室で作業

を行っていたことが認められる。

イ　被告シンフォームとＡとの間には雇用契約は締結されておらず（争いがない。）、被告シンフォームは、被告ベネッセＣｏから委託を受けた本件業務を外部の会社（１次委託先）に委託していたもので、１次委託先の会社との間で業務委託契約を締結していた（甲７５）。Ａは、本件業務に関しては、被告シンフォームからみて３次委託先の従業員であった（前記３認定事実⑴ウ）。

したがって、被告シンフォームが、Ａとの関係で、民法７１５条１項本文の「ある事業のために他人を使用する者」といえるためには、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認められることが必要である。

この点、Ａは、不正競争防止法違反の被疑事実により起訴された刑事事件（前記前提事実⑻）の公判廷において、被告シンフォームの従業員から業務上の指示を受けていたこと、加入していたグループに１次委託先の責任者が所属していないことがあったこと、１次委託先の責任者とされていた者は、Ａが多摩事務所で働き始めた頃は毎日多摩事務所に出勤していたものの、数か月後には、週に２回ないし３回の出勤となり、やがて多摩事務所に一切来なくなっていたこと、平成２４年６月頃以降になると、Ａが１次委託先の責任者とされる者から指示を受けることや、業務に関する報告を求められることはなくなり、Ａから同人に対して業務に関する報告をすることもなくなったことなどを供述している（甲６５、６６）。

しかしながら、①システムエンジニアという職務の内容及び性質に照らし、Ａが日々の作業を遂行するに当たって所属するグループの責任者に特段の指示を仰ぐ必要があったとは容易に考え難いところ、Ａ自身、本件データベースにアクセスする部分以外は、担当業務を多摩事務所ではない場所で単独で遂行することが可能であったとして、日常的な作業指示を必要

としなかったことをうかがわせる供述をしていること（甲６６）、②Ａを被告人とする上記刑事事件において、被告シンフォームの顧客分析課課長のＧ及び同事業開発本部長兼事業開発部長のＨは、Ａを含む被告シンフォームに常駐して業務を遂行する委託先等の従業員に対しては、緊急性が高い場合を除き、原則として、１次委託先の責任者を通して指示をしており、被告シンフォームの従業員が直接指示をすることはない旨供述していること（甲６８、７５）、③多摩事務所に１次委託先の責任者が不在の期間があったとしても、１次委託先の責任者又はその代行者が、被告シンフォームの執務室で業務に従事している１次委託先等の従業員（Ａを含む）に対してメールや電話で指示したり、逆に従業員の方から１次委託先の責任者又はその代行者に対してメールや電話で連絡や相談をしたりすることは容易に想定され、現にメールでのやり取りがされていた事実が認められることなど（乙２～１２）からすれば、１次委託先の責任者が多摩事務所に常駐していなかったとしても、直ちに、被告シンフォームの従業員が、直接、Ａに対し、日常の業務について個別具体的に指揮監督をしていたと認めることはできない。

また、前記３認定事実⑴イのとおり、被告シンフォームの顧客分析課内の各グループでは、毎日又は毎週、進捗会議と呼ばれる打合せが行われ、当該グループのメンバー全員（Ａを含む）が参加し、作業の進捗状況を共有していたことが認められるが、複数の委託先が関与する大規模案件の場合には、業務を効率化するために各担当者の作業の進捗状況を確認することが必要であるといえるし、そのための会議に出席して進捗状況を共有することも委託業務の内容に含まれ得るのであるから、進捗会議が開催され、Ａがこれに参加していたからといって、これをもって直ちにＡが被告シンフォームの従業員から具体的な作業指示を受けていたことを意味するものではない。

そうすると、前記アの事実は、被告シンフォームと１次委託先の会社との間の業務委託契約に基づき、１次委託先の指揮監督の下でＡの業務が行われていたことと矛盾するものではなく、被告シンフォームが、１次委託先との間の業務委託契約の範囲を超えて、Ａに対して、日常の業務につき個別具体的に指示するなど、実質的な指揮監督をしていたということはできない。

⑶　小括

以上によれば、本件漏えい行為につき、被告シンフォームが、原告らに対し、Ａを被用者とする使用者責任を負う旨の原告らの主張は、その余の点について判断するまでもなく、採用することができない。

９　争点⑻（被告ベネッセＨＤは、不法行為責任を負うか。）について

原告らは、被告ベネッセＨＤには、本件当時、保有する個人情報の利用・管理に責任を持つ部門を設置するべき注意義務（部門設置義務）があったと主張する。

被告ベネッセＨＤは、ベネッセグループを統括する立場にあったものであるから、回顧的にみれば、本件当時、同グループ内により適切な部署を設置することが、グループとしての戦略上も個人情報を提供する顧客らに対する道義上の責任からも望ましいかたちであったということはできるものの、被告ベネッセＨＤがこのような部門を設置していたからといって、本件漏えい行為を阻止し得たとは認められない。

すなわち、本件漏えい行為に関して被告シンフォーム及び被告ベネッセＣｏに認定することができる過失は、上記４及び５で認定・説示した本件セキュリティソフトの設定内容に関わる具体的な注意義務違反及び業務委託先への監督義務違反であるところ、このような具体的な注意義務違反の有無は、被告ベネッセＨＤが同グループ内に特定の部門を設置していたか否かによって影響を受ける関係にあるとは解されない。仮にベネッセＨＤに原告らの主張する部門設

置義務があると考えられるとしても、被告ベネッセＨＤは、被告シンフォーム及び被告ベネッセＣｏと別の法人格を備えた法人であって、本件業務の契約にも本件業務にも何ら関与していないのであるから、被告ベネッセＨＤが特定の部門を設置することによって本件漏えい行為という結果に影響を与えたとはいえない。

したがって、被告ベネッセＨＤが、本件漏えい行為に関して不法行為責任を負うと認めることはできない。

10　争点⑼（本件漏えい行為により原告らに損害が発生したか及びその額）について

⑴　上記２で認定したとおり、Ａの本件漏えい行為に係る被告シンフォーム及び被告ベネッセＣｏの過失行為によって、別紙６－１～５の各事件の認容原告番号目録記載の原告ら（なお、別紙７認否表の「備考」欄において被告らが情報漏えいを自認している者を含む。以下、総称して「漏えい対象原告ら」という。）について、氏名、性別、生年月日、郵便番号、住所、電話番号、メールアドレス又は保護者の氏名といった情報項目の１つ又は複数が漏えいしたことが認められる。

本件漏えい行為によって流出した顧客情報は、名簿業者３社に売却され、名簿業者３社からさらに転売されるなどして、不特定多数の者が、漏えい対象原告らの個人情報を取得したことが認められ、これらの情報が流出した範囲は広く、その回収は事実上不可能である。その結果、これらの情報を取得した者において、これらの情報を取得された漏えい対象原告らに対して郵便物の送付、メールの送付、電話をかけることなどの直接的な連絡が可能となったほか、これらの個人情報が組み合わされて悪用されることによって漏えい対象原告らの私生活上の平穏を害するおそれも生じている。

したがって、これらの情報を取得された漏えい対象原告らには、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よって、このような事態その

ものに対する不快感のみならず、不特定多数の者が自己の個人情報を取得したことが及ぼす影響に対する不安感が生じるとともに、提供した相手方である被告ベネッセＣｏ以外に提供した個人情報がみだりに開示されることがないとの信頼や期待が裏切られたことによる怒りや失望感を覚えるなどして、精神的苦痛を被ったと認めることができる。

⑵ア　前記⑴のとおり、漏えい対象原告らには、氏名、性別、生年月日、郵便番号、住所、電話番号、メールアドレス又は保護者の氏名といった個人情報が自己の了知しないところで漏えいしたことによって精神的苦痛が生じたと認めることができるものの、これらの情報は、個人を識別するために必要な情報又は個人に連絡をとるために必要な情報であり、社会生活を営む上で一定範囲の他者に開示することが予定されているものであるから、秘匿する必要性が高い情報であるとはいえない。

イ　また、本件漏えい行為により、約５００社に個人情報が流出したとの報道がされているところ（前記前提事実⑷エ）、漏えい対象原告らは本件当時あるいはそれ以降においてダイレクトメール等が増えたような気がするなどと主張しているものの、本件記録を検討しても、漏えい対象原告らの印象以上に漏えい対象原告らに財産的損害を含めたその他の実害が生じていることを認めるに足りる的確な証拠は見当たらない。

ウ　一方で、前記３認定事実⑴エによれば、被告シンフォームは、Ａ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同意書を提出させていたほか、Ａに対し、本件業務に従事させる前後において、情報セキュリティ研修等を受講させていたことが認められる。そして、前記前提事実⑸及び⑺によれば、被告ベネッセＣｏは、①本件漏えい行為の発覚後、情報漏えいの被害拡大を防止する手段を講じ、警視庁に対する捜査依頼や監督官庁に対する相談・調査報告等を行ったこと、②個人情報が漏えいしたと思われる顧客に対しては、本件通知書を送付す

るとともに、顧客の選択に応じて５００円相当のお詫びの品の交付を申し出るなどして損害の軽減に努めたことが認められる。

⑶　前記⑴によれば、漏えい対象原告らには、本件漏えい行為についての被告シンフォーム及び被告ベネッセＣｏの過失による不法行為によって、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ところ、前記⑵の事情を加味して総合的に考慮すると、漏えい対象原告らの精神的損害に対する慰謝料としては、流出した項目の多寡や、流出した情報が正確性を欠くか否かにかかわりなく、漏えい対象原告ら１人当たり各３０００円を認めるのが相当である。

そして、原告らが弁護士を訴訟代理人として本件訴訟を追行したことは当裁判所に顕著であり、本件事案の内容、損害額及びその他諸般の事情を総合考慮すれば、原告らにつき、本件漏えい行為についての被告シンフォーム及び被告ベネッセＣｏの過失による不法行為と相当因果関係のある弁護士費用として、各３００円を認めるのが相当である。

⑷　被告らは、別紙７認否表の「情報項目」欄に「△」又は「▲」の記載のある情報項目については、原告らが主張する情報項目の内容と一致するかは不明であるとし、さらに、本件漏えい行為後に姓や住所を変更した場合には損害が認められないなどと主張する。

しかしながら、本件漏えい行為によって流出した漏えい対象原告らの当該個人情報が不正確であり、あるいは、漏えい後に変動した事実があったとしても、上記⑴で説示した個人情報が流出した不快感や失望感が生じることに変わりはなく、また、流出した情報から追跡されて現在の原告らの情報に辿り着く可能性は十分に存することから、上記⑴で説示した不安感が軽減されるともいえない。

したがって、被告らの上記主張を踏まえても、漏えい対象原告らの精神的損害に対する慰謝料は各３０００円とするのが相当である。

11　まとめ

以上によれば、被告シンフォーム及び被告ベネッセＣｏは、それぞれ、原告らに対して過失による不法行為責任を負うところ、被告シンフォーム及び被告ベネッセＣｏの不法行為は、被告ベネッセＣｏが保有し、その取扱いを被告シンフォームに委託していた個人情報の管理に関するものであって、客観的に関連するものといえるから、共同不法行為（民法７１９条１項前段）の関係にある。したがって、被告シンフォーム及び被告ベネッセＣｏは、連帯して、漏えい対象原告ら（別紙６－１～５の各事件の認容原告番号目録記載の原告ら）に対して、各３３００円及びこれに対する不法行為の後の日である各事件の訴状送達の日の翌日から支払済みまで改正前民法所定の年５分の割合による遅延損害金の支払義務を負うものであり、原告らの請求は上記の限度で理由がある。

他方で、その余の原告らの請求には理由がない。

第４　結論

よって、原告らの請求は、主文１～５項の限度でそれぞれ理由があるからこれらの限度で認容し、その余の請求はいずれも理由がないから棄却することとし、訴訟費用の負担について民事訴訟法６１条、６４条本文及び６５条１項本文を、仮執行の宣言について同法２５９条１項を、それぞれ適用して、主文のとおり判決する。

東京地方裁判所民事第７部

裁判長裁判官　　新　谷　祐　子

裁判官　　坂　本　隆　一

5

裁判官　　志　村　敬　一

別紙１原告一覧表，別紙２原告一覧表，別紙３原告一覧表，別紙４原告一覧表，別紙５原告一覧表，別紙６認容原告番号目録及び別紙７認否表は記載省略