主　　文

１　被告ＢＢテクノロジー株式会社は，甲事件原告らそれぞれに対し，６０００円及びこれに対する平成１６年５月２９日から支払済みまで年５分の割合による金員を支払え。

２　被告ＢＢテクノロジー株式会社は，乙事件原告らそれぞれに対し，６０００円及びこれに対する平成１７年６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。

３　原告らの被告ＢＢテクノロジー株式会社に対するその余の請求及び被告ヤフー株式会社に対する請求をいずれも棄却する。

４　訴訟費用の負担は以下のとおりとする。

(1)　原告らに生じた費用の２分の１と被告ＢＢテクノロジー株式会社に生じた費用の合計額のうち，１０分の１を同被告の負担とする。

(2)　(1)を除く全ての費用は原告らの負担とする。

５　この判決は，第１，２項に限り仮に執行することが出来る。

事　実　及　び　理　由

第１　請求

１　被告らは，甲事件原告らそれぞれに対し，各自１０万円及びこれに対する平成１６年５月２９日から支払済みまで年５分の割合による金員を支払え。

２　被告らは，乙事件原告らそれぞれに対し，各自１０万円及びこれに対する平成１７年６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

本件は，インターネット接続等の総合電気通信サービスである「Ｙａｈｏｏ！ＢＢ」の会員であった原告らが，同サービスの顧客情報として保有管理されていた原告らの氏名・住所等の個人情報が外部に漏えいしたことについて，共同して同サービスを提供している被告らが個人情報の適切な管理を怠った過失等により，自己の情報をコントロールする権利が侵害されたとして，被告ら

に対し，共同不法行為に基づく損害賠償として慰謝料等の支払を求めた事案である。

1　争いのない事実等（争いのない事実を除き，認定に用いた証拠は括弧内に示す。）

(1)　当事者

ア　原告らは，いずれも「Ｙａｈｏｏ！ＢＢ」と称する，非対称加入者線伝送（ＡＤＳＬ）方式等を用いたインターネット接続サービス及びこれに付随するメールサーバーのレンタル等の総合電気通信サービス（以下，「本件サービス」という。）の会員である。

イ　被告らは，「Ｙａｈｏｏ！ＢＢ」の統一名称を用いて，電気通信事業法にいう電気通信事業に当たる本件サービスを顧客に対して提供している株式会社である（乙３）。

(2)　原告らはいずれも平成１６年１月までに，被告らそれぞれとの間で，本件サービスに係る契約を締結し，本件サービスに入会した。

(3)　本件サービスに係る契約締結の際に，被告らは，原告らを含む顧客それぞれの住所・氏名等の個人情報を取得し，顧客に関して，以下の情報を保有し，管理していた。

ア　被告ＢＢテクノロジー株式会社（以下，「被告ＢＢテクノロジー」という。）

住所・氏名・電話番号・メールアドレス・ヤフーメールアドレス・ヤフーＩＤ・申込日・性別・回線タイプ等の回線の接続に関する情報。

イ　被告ヤフー株式会社（以下，「被告ヤフー」という。）

住所・氏名・電話番号・メールアドレス・ヤフーメールアドレス・ヤフーＩＤ・申込日・クレジットカード番号・銀行口座番号・パスワード・取引実績に関する情報。

(4)　被告ＢＢテクノロジーにおいては，従業員が利用する端末（クライアン

ト）とは別に，被告ＢＢテクノロジー本社の施設内にサーバーを設置していた。(3)アの顧客情報は，顧客データベース（以下，「本件顧客データベース」という）に記録されており，これは，被告ＢＢテクノロジーのサーバーの一つ（以下，「本件顧客データベースサーバー」という。）に格納されていたものである。これらのデータベースを格納するサーバーでは，ＯＳ（基本ソフト）は，ほとんどが米マイクロソフト社製Ｗｉｎｄｏｗｓのサーバー用ＯＳを使用していた。

(5)　リモートメンテナンスサーバーの設置

被告ＢＢテクノロジーは，平成１４年１２月，社外のパソコンから社内のサーバーのメンテナンス作業を可能とするためのリモートメンテナンスサーバー（以下，「本件リモートメンテナンスサーバー」という。）を設置し，これにより被告ＢＢテクノロジーのサーバーに，社外からインターネットを通じてアクセスすること（以下，「リモートアクセス」という。）が可能となった。

(6)　リモートアクセスの手法

ア　リモートメンテナンスサーバーには，米マイクロソフト社のＷｉｎｄｏｗｓのサーバー用ＯＳが導入されており，インターネットを通じてリモートメンテナンスを行う方法には，サーバー用のＷｉｎｄｏｗｓが標準で備えている「ターミナルサービス」という機能が用いられた。

イ　ターミナルサービスとは，ＷｉｎｄｏｗｓがインストールされたクライアントＰＣから，クライアントソフトウェア（無償）を起動して，ＬＡＮなどのネットワークを通じてサーバーを遠隔操作することを可能にする機能である。

現在市販されているパソコンのほとんどで使われているクライアント向けＷｉｎｄｏｗｓの最新版であるＷｉｎｄｏｗｓＸＰには，ターミナルサービスからサーバーに必要な機能を省略した「リモートデスクトップ接

続」というソフトウェア（以下，「リモートデスクトップ」という。）が標準でインストールされており，ＷｉｎｄｏｗｓＸＰであれば，追加のソフトウェアを入手することなくターミナルサービスを利用することが可能となっている。

ウ　リモートデスクトップを用いて本件リモートメンテナンスサーバーに接続する際には，接続先である同サーバーのＩＰアドレスを特定した上で，ユーザー名とパスワードを正しく入力すれば，同サーバーに，ユーザー認証を受けてログオンすることが可能であり，一旦リモートデスクトップによるログオンを行ってしまえば，社外からネットワークを介していても社内で当該サーバーを直接操作しているのと全く変わらない状態となる。

エ　本件リモートメンテナンスサーバーへログオンした後，本件リモートメンテナンスサーバーから，さらにリモートデスクトップを用いて，本件顧客データベースサーバー等へログオンすることができるが，その場合，当該サーバーに接続するためのユーザー名・パスワードが必要である（甲１１の４）。

(7)　本件リモートメンテナンスサーバー等のユーザー名及びパスワード

本件リモートメンテナンスサーバーには，ログオンするためのユーザー名とパスワードとして，ユーザー名「ｇｅｎｂａｔａｉ」・パスワード「ｇｅｎｂａｔａｉ」が設定されており（以下，併せて「本件アカウント」という。），これは，社外からサーバーのメンテナンス業務を行う複数の担当者に与えられていた。

本件アカウントは，本件顧客データベースサーバーを含め被告ＢＢテクノロジーが管理する複数のサーバーについて，各種メンテナンスのために必要なファイル操作や設定変更，データやプログラムの変更を行う権限があるものとして登録されていた。

(8)　本件顧客情報の不正取得

ア　Aは，平成１４年５月１６日から，平成１５年２月末日までの間，被告ＢＢテクノロジーの業務委託先から同被告に派遣され，本件顧客データベースのメンテナンスや，同被告のサーバー群の管理を行う業務に従事していた者である（甲１０の１，１８の２）。

Aは，社外からメンテナンスを行う担当者の一人であり，本件アカウントを与えられていた。

イ　Aは知人のBと共に，平成１５年６月，本件アカウント等を使用して，インターネットカフェのパソコンからターミナルサービスを利用してリモートメンテナンスサーバーにログオンした上で，本件顧客データベースサーバーにアクセスし，本件顧客データベースに含まれる顧客情報を外部に転送し，Bが持ち込んだハードディスクに保存して不正に取得した（以下，この際の不正取得を「６月の不正取得」という。）。

ウ　Bは，平成１６年１月，再度，同様の手法で，被告ＢＢテクノロジーの保有する顧客情報を不正に取得した（以下，この際の不正取得を「１月の不正取得」，イ，ウの不正取得を併せて「本件不正取得」という。）。

エ　Aが被告ＢＢテクノロジーでの業務を終える（以下，Aの同被告における業務の終了を「退職」ともいう。）際に，被告ＢＢテクノロジーは，本件アカウントを含め，Aが利用し又は知り得たユーザー名の削除やパスワードの変更を行わず，本件リモートメンテナンスサーバーを設置した平成１４年１２月から平成１６年１月まで，本件リモートメンテナンスサーバーに設定されていたユーザー名についてパスワードの定期的変更を行わなかった。

(9)　本件不正取得に係る被告ＢＢテクノロジーの顧客情報は，Bを通じて，恐喝の実行犯であるCらに渡り，Cが，被告ＢＢテクノロジー及び関連会社であるソフトバンク株式会社に対する恐喝未遂事件（以下，「本件恐喝未遂事件」という。）で検挙された際に，本件不正取得の事実が判明した。

(10)　Ｃが取得した被告ＢＢテクノロジーの顧客情報には，原告らの個人情報が含まれており，その内容としては，①住所②氏名③電話番号④メールアドレス⑤ヤフーＩＤ⑥ヤフーメールアドレス⑦申込日を含むものであった（乙７の６，乙７の７）。

２　争点

(1)　被告ＢＢテクノロジーの過失の有無

（原告らの主張）

ア　個人情報の管理に関する一般的な注意義務

被告ＢＢテクノロジーは，その事業に原告らの個人情報を利用しているところ，これらの個人情報を適切に管理し，漏えいすることのないよう対策をする信義則上の義務を負っている。

また，被告らは，社会のインフラを提供するインターネットサービスプロバイダーの事業者として，業務上管理する個人情報の管理につき，一般企業よりも重い注意義務を負っている。本件サービスは，電気通信事業に該当するところ，電気通信事業者に対しては，個人情報の保護に関する法律（以下，「個人情報保護法」という。）が成立する以前より，個人情報保護に関する各種ガイドラインが定められており，被告ＢＢテクノロジーは，これらに基づき，社内の情報漏えいを防止する適切な措置を講じる義務を有していた。

イ　リモートアクセスに関しての注意義務違反

（ア）　現代のＩＴ社会において，企業活動にコンピュータの利用は不可欠であるが，まさに被告らが企業活動として行っているような急速なブロードバンドの普及によりインターネットへ接続する人口が急増し，これに伴い，インターネットに接続することに伴う脅威も増加・深刻化していることは周知のとおりである。

被告ＢＢテクノロジーにおいては，平成１４年１２月以前は，サーバ

ー管理を担当する者が，インターネットを通じて外部から管理を行うことは一切許可されていなかった。被告ＢＢテクノロジーは，１(5)のとおり，平成１４年１２月に本件リモートメンテナンスサーバーを設置し，リモートアクセスを可能にしたものであるが，リモートアクセスを可能にすること自体，情報漏えいの危険を高める行為であり，その危険性に鑑みて，リモートアクセスについては，ＪＩＳ規格などで各種の規定がなされているところである。

したがって，リモートアクセスを可能にするには，リモートアクセスすることの必要性がある場合に，必要な範囲に限って，相当な措置を施した上でのアクセスが許されると解するべきである。

（イ） リモートアクセスの必要性とその範囲

ａ 多数の会員に関する重大な個人情報を大量に含む本件顧客データベースを，その従業員にインターネットを通じて操作させることはこれ自体危険なことであり，情報セキュリティの確保の点から厳に慎まなければならない。

被告ＢＢテクノロジーのシステムの障害が深夜・休日を問わず発生するとしても，このような事態は業務に付随して当然予想できることに過ぎず，担当者の常駐等で十分対応できる事項である。本件サービスは，大規模に業務を展開していたのであり，個人情報が漏えいした時の危険性に鑑みれば，リモートアクセスを可能とするには強度の合理性を必要とするところ，そのような合理性は一切なかった。

ｂ また，第三者による冒用のおそれがあることから，リモートアクセスでユーザーが利用するサービスは，メールサービスや特定のサーバーへのアクセスなどに限定されるのが普通である。リモートアクセスにおいて，ユーザー名に管理者権限を付与すれば，サーバーに関するあらゆるデータの削除・複製だけでなく，ユーザー名の付与や，抹消

まで可能であり，管理者権限のあるユーザー名とパスワードが漏えいした場合に，セキュリティに壊滅的な危機をもたらしかねないから，特段の事情なくリモートアクセスのユーザー名に管理者権限を付与することは許されない。

本件アカウントは，本件リモートメンテナンスサーバーに対する管理者権限を有し，また，本件リモートメンテナンスサーバーを経由して管理の対象となる全ての被告ＢＢテクノロジーのサーバーに対する管理者権限も有していた。このような強大な権限を有するユーザー名をリモートアクセスで許容していたのは，余りにも無謀かつ危険である。

（ウ） 相当な措置

被告ＢＢテクノロジーは，以下のとおり，リモートアクセスを可能にする際の相当な措置を採っていなかったものである。

a　ファイアーウォール等によるアクセス規制

被告ＢＢテクノロジーは，外部から本件リモートメンテナンスサーバーへのアクセスに際して，ファイアーウォール等を利用して，あらかじめ登録しておいた特定のコンピュータからの接続しか受け付けない等，権限ある者による正当なアクセスのみを許容するアクセス規制を一切行っていなかった。

１(6)ウのとおり，被告ＢＢテクノロジーは，本件リモートメンテナンスサーバーのＩＰアドレスさえ判明してしまえば，何らのアクセス規制を受けることなく，インターネットカフェ内のパソコン等，世界中のどこからでも本件リモートメンテナンスサーバーへログオン認証を試みることが可能な状況を作出していた。

b　ユーザー名・パスワード管理

被告ＢＢテクノロジーは，前記のとおり，管理者権限を有する本件

アカウントが冒用されてしまった場合の危険性に鑑み，本件アカウントを含む本件リモートメンテナンスサーバーのユーザー名・パスワード管理について以下の措置をとるべきであったが，これを怠った。

（ａ） 本件アカウントの共有

被告ＢＢテクノロジーは，本件リモートメンテナンスサーバーの利用者のユーザー名とパスワードは利用者ごとに管理して厳格に共有を禁止するべきであった。

しかし，被告ＢＢテクノロジーにおいては，サーバーコンピューターの構築と運用・メンテナンス等の作業を行うＡら６名のメンバーによる「現場隊」と呼ばれるグループがあり，被告ＢＢテクノロジーは，本件アカウントを「現場隊」のメンバーに与えていた。また，「現場隊」のメンバー以外にも，サーバーコンピュータに携わる従業員には，本件アカウントの使用を認めていた。

（ｂ） 本件アカウントの品質

被告ＢＢテクノロジーは，ユーザー名・パスワードについて解析されにくい強度のものを使用すべきであったが，本件アカウントは「現場隊」という日本語として読めること，ユーザー名とパスワードが同じであるなど，品質の低いものであった。

（ｃ） 退職時の変更

被告ＢＢテクノロジーは，本件アカウントを含むＡが利用し又は知り得たユーザー名・パスワード等について，退職後に悪用されないようユーザー名の削除又はパスワードの変更をすべきであった。

本件においては，サーバー群の管理を行っていた現場隊の構成メンバーは，同被告のネットワークを熟知していたのであるから，Ａのように現場隊のメンバーが異動・退職した場合には，同被告は，少なくともその者が現場隊に所属していた時と同じ権限を行使でき

ないような対策をとるべきであったことは明白であった。

しかし，本件においては，被告ＢＢテクノロジーは，１(8)エのとおり，Ａが退職した後も，本件アカウント等を何ら変更することなく長期間放置していた。

（ｄ） 定期的な変更

被告ＢＢテクノロジーは，本件リモートメンテナンスサーバーに設定されたユーザー名について定期的にパスワードの変更をすべきであったところ，１(8)エのとおりこれを行わなかったものである。

（ｅ） 不正侵入発覚後の措置

被告ＢＢテクノロジーは，平成１５年１２月末ころに，Ｂが行った本件リモートメンテナンスサーバー等に対する不正アクセスに気付いた際に，それらの運用を停止するか，最低限，本件アカウントを含め，現存していたユーザー名を全て破棄すべきであったところ，そのような対策をとらず，Ｂによって変更されたパスワードを変更前のものに戻している。

ウ　本件不正取得についての予見可能性及び結果回避可能性

（ア） 予見可能性

Ａは，１(8)アのとおり，平成１５年２月末日に被告ＢＢテクノロジーを退職したが，退職の直前にＡと同被告との間に何らかのトラブルがあったか，少なくともＡにとって同被告を退職することは，極めて不本意なものであったことが強く推測される。このような状況においては，被告ＢＢテクノロジーは，同被告に不平を持っていたＡが退職後に本件アカウントやその他Ａが知り得たユーザー名・パスワードを用いて本件リモートメンテナンスサーバーへのアクセスを行うことを予見し，又は予見可能であったというべきである。

また，本件が犯罪行為であるから予見不可能であるということはでき

ない。

（イ） 結果回避可能性

被告ＢＢテクノロジーにおいて，Ａの知り得たユーザー名を全て削除したり，ファイアーウォール等によりアクセス制御を施す等の措置をとることで，Ａによる本件リモートメンテナンスサーバーへのアクセスを防止することは可能であった。

エ 以上のとおり，被告ＢＢテクノロジーは，保有する個人情報を適切に管理し，その漏えいを防ぐために適切な措置を講ずべき注意義務を怠ったものであり，その過失により原告らの個人情報が漏えいしたのであるから，原告らに対して不法行為責任を負う。

（被告ＢＢテクノロジーの主張）

ア 被告ＢＢテクノロジーが，個人情報についての管理義務に違反し，この過失により原告らの個人情報が漏えいしたとの主張については争う。

イ リモートアクセスに関する注意義務違反

（ア） 原告らも主張するとおり，リモートアクセスについては，リモートアクセスすることの必要性がある場合に，必要な範囲に限って，相当な措置を施した上でのアクセスは許されると解すべきであるところ，本件当時の被告ＢＢテクノロジーにおいては，リモートアクセスする必要があり，必要な範囲に限って，相当な措置を講じた上で，リモートアクセスを認めていたものである。

（イ） リモートアクセスの必要性とその範囲

ａ 被告ＢＢテクノロジーが管理していた本件顧客データベースには何百万件もの個人情報が記録されており，単なる住所・氏名だけではなく，本件サービスの提供に必要な電話回線の回線タイプや接続先であるＮＴＴ局舎名等の顧客が使用する接続に関する情報も記録されている。また，日々加入した顧客を新規登録する必要があり，住所変更や，

電話番号変更等，本件顧客データベースに登録されている情報が変更された場合には，即座にそれらの情報を変更する必要があるので，ひとたび本件顧客データベースを含むシステムに不具合が生じた場合に，至急対応して復旧しなければ顧客に対するサービスを提供することができない。

顧客データベースを含む被告ＢＢテクノロジーのシステムは２４時間常に稼働しており，システムトラブルは，当然，深夜・休日など時間を問わず発生するため，外部からでもメンテナンスを行うためリモートアクセスの必要性があった。

b　１(7)のとおり，本件アカウントには，被告ＢＢテクノロジーが管理するサーバーについてメンテナンス等を行う権限が与えられていたが，これは被告ＢＢテクノロジーが管理するサーバー全体の５分の１強のサーバーについてであり，本件アカウントに全てのサーバーの管理者権限が与えられていた訳ではない。

本件アカウントに，被告ＢＢテクノロジーが管理するサーバーのメンテナンスに必要なファイル操作や設定変更，データやプログラムを変更する権限を与えていたのは，２４時間体制で，社外からもメンテナンス業務を行うためのものであるから当然である。

（ウ）　相当な措置

a　ファイアーウォール等によるアクセス規制

被告ＢＢテクノロジーにおいても，本件リモートメンテナンスサーバーへのアクセスについては，ユーザー名とパスワードによる認証を行っており，何らのアクセス規制もなく，本件リモートメンテナンスサーバーに接続を試みることはできなかった。

また，本件リモートメンテナンスサーバーのＩＰアドレスを第三者が特定することは困難である。

ｂ　ユーザー名・パスワード管理

（ａ）　本件アカウントの共有

本件リモートメンテナンスサーバーに接続できる人数については，１３人に限られており，ユーザー名等は，被告ＢＢテクノロジーの担当者によって管理されていたものである。

本件当時は，個人情報保護法も施行されておらず，現在ほど各企業ともに個人情報の管理を厳密に行っていなかったのであり，ユーザー名を共有しないことは義務づけられていなかった。

（ｂ）　本件アカウントの品質

「現場隊」という名称については，メンテナンス業務を行うために組織されたチームの通称にすぎず，被告ＢＢテクノロジー社内の一部のもので知られているにすぎなかったものであるから，「ｇｅｎｂａｔａｉ」という本件アカウントについて，外部の者が簡単に類推できるようなものではなかった。

（ｃ）　退職時の変更

従業員個人に与えたユーザー名について，退職後速やかに抹消すべきことについては認める。

ただ，本件当時のガイドラインにおいては，アクセス権限者が異動した場合や退職した場合にユーザー名を直ちに無効にするべきであるとまでは規定されていなかったものである。

（ｄ）　定期的な変更

１(8)エのとおり，被告ＢＢテクノロジーは，約１年間，ユーザー名及びパスワードの定期的な変更をしなかったことは認めるが，これをもって過失ということはできない。

（ｅ）　不正侵入発覚後の措置

被告ＢＢテクノロジーは，何者かによって改ざんされた本件アカ

ウントを平成１６年１月８日に使用停止にしている。

ウ　本件不正取得についての予見可能性及び結果回避可能性

（ア）　本件不正取得は，通常の情報管理体制によっては，防御しようのない社外の第三者の犯罪行為という特異な事情によるものである以上，被告ＢＢテクノロジーにおいては予見可能性及び結果回避可能性がなく，過失はない。

（イ）　予見可能性

従業員や派遣社員が会社に対して不平を抱いていたことから，被告ＢＢテクノロジーが，不正アクセス等の犯罪行為が行われることを予見し，又は予見可能であったとすることはできない。

（ウ）　結果回避可能性

本件においては，侵入に用いられたのは本件アカウントのみではなく，Ａ及びＢが，本件アカウントを利用して顧客データベースにアクセスし，原告らの個人情報を持ち出しているかは明らかではない。平成１６年１月１３日に個人情報が不正に取得されるに先立ち，同月８日には，被告ＢＢテクノロジーは，何者かによって改ざんされた本件アカウントを使用停止にしている。したがって，本件アカウントを厳重に管理していたとしても，Ａによる不正アクセスを防止することは困難であった。

(2)　被告ヤフーの責任の有無

（原告らの主張）

ア　管理義務違反に基づく不法行為責任

被告ヤフーは，被告ＢＢテクノロジー同様，個人情報についての管理義務に違反した過失があり，この過失により，被告ヤフーの管理する原告らの個人情報が漏えい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　監督義務違反等に基づく共同不法行為責任

仮に，原告らの個人情報を含む顧客情報について，被告ヤフーの主張するとおり，被告ＢＢテクノロジーと被告ヤフーが別個に管理し，被告ヤフーが管理していた情報が，一切持ち出されていないとしても，以下の点で，被告ヤフーに過失が認められ，被告ＢＢテクノロジーと共同不法行為責任を負う。

（ア） 被告らはいずれもソフトバンク株式会社の子会社であり，ソフトバンクグループに属している。被告ヤフーは，被告ＢＢテクノロジーと一体となって顧客と本件サービスの契約を締結している当事者であり，外形的に一体となって本件サービスを提供しており，本件サービスの顧客の情報についても利用料金の徴収等で一体の利用環境にあったものである。

このような本件サービスの全体から合理的に考えれば，被告ヤフーと被告ＢＢテクノロジーは一体として個人情報を適切に管理する義務を負っており，受領した個人情報を被告ヤフーのサーバーに保存しているか，被告ＢＢテクノロジーのサーバーに保存しているかは，被告ら内部での職務分掌にすぎない。したがって，被告ヤフーは，自己の管理するサーバだけではなく，被告ＢＢテクノロジーの管理するサーバーに保存されている個人情報についても適切に管理する義務があった。

また，少なくとも，被告ヤフーは，被告ＢＢテクノロジーが個人情報を適切に管理するように監督する作為義務を負っていたものである。

（イ） 本件では，原告らは，被告ら両者との間で，本件サービスを受けるための契約を締結するとともに，その利用に必要な個人情報の管理を委託する旨合意し，被告らから不可分一体のサービスの提供を受けて，その対価である利用料金を被告ヤフーに対して払っている。

被告らの会社の沿革，資本関係，共同して本件サービスを提供し，顧客に対し，外形上被告らが一体として認識されていることに鑑みれば，

被告らに客観的関連共同性が認められることは明らかである。

（被告ヤフーの主張）

ア　管理義務違反に基づく不法行為責任

被告ヤフーと被告ＢＢテクノロジーは，法人格が異なるのはもちろんのこと，被告ＢＢテクノロジーが回線等のハード面のサービスを提供し，被告ヤフーがホームページ等のソフト面のサービスを提供しており，別個独立のサービスを「Ｙａｈｏｏ！ＢＢ」の統一名称を用いて行っているに過ぎない。

被告ヤフー及び被告ＢＢテクノロジーは，必要となる顧客情報が異なることから，原告らの個人情報を含む顧客情報（内容は１(3)のとおり）を別のサーバーに別個に管理しており，共有しているわけではない。被告ヤフーが保有していた顧客情報は，一切，外部に持ち出されていない。

イ　監督義務違反等に基づく共同不法行為責任

原告らの主張は，否認ないし争う。

(3)　権利侵害の有無

（原告らの主張）

ア　被告らの不法行為により，原告らの個人情報を含む大量の個人情報の漏えいという重大な結果を招き，原告らの自己の情報をコントロールする権利（自己情報コントロール権）が侵害されている。

また，本件のＢによる情報漏えいについては，Ｂは，当初から恐喝を目的として顧客情報を取得しておらず，顧客情報を取得した後に，当該顧客情報の処分先として紹介されたＤが恐喝を企図し，Ｃらと共謀するに至ったという事案であるから，仮に，捜査機関により原告らの個人情報が記録されたＤＶＤ－Ｒ等が押収されるなどしていたとしても，自己の情報が得体の知れない反社会的集団の手に渡ったこと自体が，原告らの自己情報コントロール権の侵害である。

イ　二次流出について

（ア）　本件においては，Ａ及びＢとは無関係な第三者であるＤやＣら本件恐喝未遂事件の関係者に，Ｂを通じて，原告らの個人情報を含む顧客情報が渡ったこと自体が二次流出というべきである。

（イ）　また，原告らの個人情報を含む被告ＢＢテクノロジーの顧客情報が記録されたＤＶＤ－ＲとＣＤ－Ｒを受け取ったＤがこれをＣに渡した後，当該ＤＶＤ－ＲとＣＤ－Ｒがいかなる経過をたどったのかについては不明である。この点，喝取金の受領を確実にするため原本以外にコピーを作成・保管しておくのは恐喝の常套手段であり，デジタルデータは容易に複製が可能であることからすれば，本件のような恐喝事案では，個人情報が何らかの手段で複製された可能性が高いというべきであり，結局，本件不正取得によって漏えいした個人情報がすべて回収されたという確証はない。

（ウ）　また，平成１６年末ころ，被告ＢＢテクノロジーの顧客情報が出版社に持ち込まれたり，インターネットのホームページ上で公開されたりするという事件が発生したと報道されており，被告ＢＢテクノロジーも，流出した情報については，平成１５年３月１１日から同月２２日時点における同社の顧客情報の一部と符合すること，及びその母数が約８万６０００件であったとのプレスリリースを出しており，本件不正取得に係る顧客情報が本件恐喝未遂事件の関係者以外に一般に流通していた疑いは極めて強い。

（被告らの主張）

原告らの主張は否認する。

ア（ア）　個人情報については，その情報内容について，現に文字としてモニターに表示されるか，又は，プリントアウトされるなどして直ちに情報の意味内容を第三者が読みとれる状態（認識可能な状態）で開示されて

初めて，当該個人の権利が侵害されたというべきである。

（イ） 本件では，被告ＢＢテクノロジーから顧客情報のデータを持ち出したＡ及びＢは，そのデータをハードディスク，ＣＤ－Ｒ，ＤＶＤ－Ｒといった媒体に記録したまま保有しており，Ｃが恐喝に用いるためにプリントアウトした極めて一部の顧客に関する情報を除いて，原告らの個人情報を含め，一度も外部から認識可能な状態に置かれたことはなく，Ａや恐喝犯らを含め原告らの個人情報を現に認識した者もおらず，このような状態で，原告らの権利が侵害されたとはいえない。

Ｂが被告ＢＢテクノロジーから不正に持ち出した顧客情報は，ＣＤ－Ｒ，ＤＶＤ－Ｒといった媒体に保存された状態のまま，Ｂの共犯者であるＥ，Ｄ，Ｃの手に渡っているだけであり，外部の第三者はもちろんのこと不正取得した犯人たちでさえ原告らの情報を読みとることがないまま，後述のとおり，当該情報が記録された記録媒体は破棄されるなどしている。上記記録媒体には，原告ら以外の顧客の情報も含め合計数百万人分もの顧客のデータが記録されていたのであるから，実際上，原告らを含む個々の顧客の個人情報が着目され，個別に認識されることなど到底あり得なかった。

（ウ） また，上記のとおり，本件においては，原告らの私的事項が一切「公表」，「開示」されていないことから，原告らのプライバシーの権利が侵害されたともいえない。

イ　二次流出について

（ア） 被告ＢＢテクノロジーが，顧客情報のデータが外部に持ち出されたことを迅速に発表したため，犯行の発覚をおそれたＡ及びＢは，それぞれ顧客情報のデータを破壊し，顧客情報の入っていたハードディスクを破棄した。また，ＢがＤに渡したＣＤ－ＲとＤＶＤ－Ｒは警察に領置され，既に回収されているのであって，現在に至るまで二次流出は確認さ

れていない。

（イ） 被告ＢＢテクノロジーが，原告らの主張するプレスリリースを出したことは認めるが，原告らのデータは，前記の最大８万６０００件の個人情報の中には含まれていない。

また，マスコミに持ち込まれた経緯や，インターネットに流出した経緯については不明であり，Ａ・Ｂによる情報漏えい事件によって漏えいしたものであるとの裏付けはない。

(4) 損害

（原告らの主張）

原告らには，自己情報コントロール権が侵害されたことそれ自体に対する精神的苦痛及び不特定の第三者にいついかなる目的でそれが利用されるか分からないという不安感という精神的苦痛を受けており，これに基づく精神的損害が生じていることは明らかである。

今回漏えいした情報は，個人を特定し，また，本人と連絡を取るために不可欠な情報であり，現在，実在するメールアドレスや電話番号は，架空請求などのために利用されていることが問題となっている。原告らは，今後，架空請求や詐欺等の被害に怯えて暮らさなければならず，原告らに対する架空請求等の実際の被害の発生の有無にかかわらず，その不安感だけでも精神的負担・損害は甚大である。

よって，原告らが被った損害は，１人あたり慰謝料１００万円，弁護士費用としてその２４％相当額の２４万円の合計１２４万円は下らない。

原告らは，全損害の内金として，請求の趣旨記載の金員（一人あたり１０万円）の支払を求める。

（被告らの主張）

原告らの主張は，否認する。

原告らの主張は，広範囲に個人情報が出回っている可能性が高いことを前

提とするものであるが，前記のとおり，本件では原告等の個人情報が二次流出したとの事実はない。原告らの主張は，外部に不正に持ち出された顧客情報がすべて回収された確証がなく漠然たる不安があると述べるものであって，原告らに損害はない。

また，本件において，漏えいした原告らの個人情報としては，氏名，住所，電話番号，メールアドレス程度の基礎的な情報しか記録されていなかったのであり，その持ち出しが直ちに損害を構成するものではない。

第３　判断

１　本件不正取得の経緯等

前記の争いのない事実等に証拠（甲１０の１～２，１１の１～５，１２，１３の１～４，１４～１６，１８の１～７，１９の１～１１，２０の１～２８，２４の１～１２）及び弁論の全趣旨を総合すれば，本件不正取得の経緯等について，以下の事実が認められる（認定事実の末尾に，当該事実の認定に用いた主な証拠を掲記する。）。

(1)　被告ＢＢテクノロジーのサーバー管理体制

ア　現場隊

被告ＢＢテクノロジーにおいては，平成１４年１１月末頃に，本件顧客データベースサーバーのデータにトラブルが発生したことが契機となり，同年１２月ころ，社内に，同社の従業員であるＦをリーダーとして，Ａを含む合計６名のメンバーで構成される通称「現場隊」というグループを発足させた（甲１１の２，１１の５，１８の２，１８の６）。

現場隊の業務は，被告ＢＢテクノロジー内のデータベース等のサーバーコンピュータの構築と運用，メンテナンス，サーバーコンピュータ内の記録データのバックアップ作業等，多岐に渡り，情報処理本部が使用していた５０台以上のサーバーを管理していた（甲１１の２，１１の５）。

イ　リモートメンテナンスサーバーの設置

（ア） 本件リモートメンテナンスサーバーが設置される以前は，被告ＢＢテクノロジーにおいては，社内ネットワークの一部にはインターネットを通じてアクセスできるようにしていたが，セキュリティの関係で，インターネットを通じてアクセスした場合にデータベースの入ったサーバーには，アクセスができないようにしていた（甲１１の１）。

（イ） 現場隊の業務は，顧客や各部署からの要望に常時対応する必要があり，被告ＢＢテクノロジーは，平成１４年１２月２７日，本件リモートメンテナンスサーバーを設置し，顧客データベースへのリモートアクセスを認めることになった。これは，夜間や休日に緊急にサーバーのメンテナンスの必要が生じた場合に社外からインターネットを通じてサーバーのメンテナンスを行う目的で，年末年始の休みが近づいていたことから設置されたものであった（甲１１の１，１１の５，１３の２）。

（ウ） なお，本件リモートメンテナンスサーバーのほかに，被告ＢＢテクノロジーは，サーバー群を監視するためのサーバーを一台設置しており（以下，「本件監視サーバー」という。），平成１５年２月ないし３月ころから，本件監視サーバーに対しても，リモートデスクトップを用いて，外部からログオンすることが可能であった（甲１１の３，１１の５，１３の１）。

ウ 本件リモートメンテナンスサーバーへのアクセスの許可状況

平成１６年１月１２日までに，本件リモートメンテナンスサーバーに登録されていた利用者の総数は６５名であり（甲１３の２），登録されているユーザー名には，本件アカウントを含め，ユーザー名とパスワードが同じものが多数存在していた（甲１８の２～３，２０の２２）。

エ 本件アカウントの権限

（ア） 本件アカウントには，本件リモートメンテナンスサーバーの管理者権限（アドミニストレータ権限）が与えられていた。

管理者権限は，サーバーについて，データの消去や変更，アカウントの追加登録作業，各種設定追加変更，ハードウェアのメンテナンス，障害監視等が行える権限であり，現場隊の業務として，サーバーのハードウェアのメンテナンス，障害監視等があったため，本件アカウントに管理者権限が与えられていたものであった（甲１１の２，１３の２）。

（イ） また，本件リモートメンテナンスサーバー同様に，現場隊がメンテナンスしていた各サーバーコンピュータにも，管理者権限が与えられたユーザー名として本件アカウントを登録することが認められていた（甲１１の２，１３の２）。

（ウ） 本件アカウントは，現場隊のメンバーがグループで使用していたグループアカウントであるが，現場隊以外には，サーバーに携わる社員に限り，サーバーのメンテナンスのために本件アカウントを利用することが認められており，平成１６年１月３０日までに，延べ１３名がこの使用を認められていた（甲１３の２）。

なお，Ａ個人に対しては，本件リモートメンテナンスサーバーのユーザー名とパスワードは与えられていなかった（甲１１の１，１８の２）。

（エ） 本件アカウントで本件リモートメンテナンスサーバーにログオンした場合には，同サーバーに登録されているユーザー名の一覧を確認することができ，それらの削除等を行うことができた。また，本件アカウント以外で本件リモートメンテナンスサーバーにログオンした場合にも，登録されているユーザー名の一覧を確認することができた（甲２０の２５，２０の２８）。

オ 本件顧客データベースの保管状況

（ア） 本件顧客データベースの原本は，本件顧客データベースサーバーに保管されていた。また，Ａが，被告ＢＢテクノロジーで業務を行っていた際に，本件顧客データベースのバックアップを採ったデータを，別の

サーバー（以下，「旧バックアップサーバー」という。）に保管していたことがあった。

本件不正取得当時は，毎日，データのバックアップを採って，最新のデータを本件リモートメンテナンスサーバーの中に保存しており，旧バックアップサーバーは使用されていなかったが，稼働はしていた。

Ａは，被告ＢＢテクノロジーで業務を行っていた際，本件顧客データベースサーバー及び旧バックアップサーバーのメンテナンス業務を担当していた（甲１２，１４，１８の１）。

（イ） 本件顧客データベースサーバーのユーザー名について

本件顧客データベースサーバーには，データベース管理用のユーザー名（以下，「本件データベースアカウント」という。）が本件アカウント以前から設定されており，Ａはこれを知っていた。

本件顧客データベースサーバーにも，本件アカウントは登録されていた（甲１８の３，１８の６～７）。

(2) ６月の不正取得

ア Ａは，退職後の平成１５年５月ころ，被告ＢＢテクノロジーのサーバーから，本件顧客データベースのデータを取得することを考え，知人のＢに相談した（甲１８の１）。

Ｂは，相談された当初は乗り気ではなかったものの，次第に興味を抱き，同月末ころ，Ａと共に被告ＢＢテクノロジーのリモートメンテナンスサーバーへ侵入することに合意した（甲１８の１，２０の２，２０の１６）。

両名は，この計画を行うに際して，身元が判明しないようにするためインターネットカフェのパソコンを利用すること，利用者に対する監視や身分確認が甘い店舗を選択すること，侵入に際してはグローバルＩＰアドレスが付与されたパソコンで行う必要があること等を打ち合わせた（甲２０の２，２０の２１。）

イ　本件顧客データベースのデータの取得経緯

Ａは，Ｂと共に，同年６月１３日，同月２０日，同月２７日，インターネットカフェに赴き，被告ＢＢテクノロジーのサーバーにアクセスした。本件顧客データベースサーバー内から本件顧客データベースのデータをＡらが取得した経緯は，以下のとおりである。

（ア）　６月２０日のアクセス

ａ　６月２０日，Ａは，Ｂと共に，インターネットカフェに行き，店内のパソコンから，リモートデスクトップを用いて，本件リモートメンテナンスサーバーのＩＰアドレス及び本件アカウントを入力して，本件リモートメンテナンスサーバーにログオンした（以下，リモートデスクトップを用いて，接続先のサーバーを特定し，ユーザー名とパスワードを入力してサーバーにログオンすることを，単に「サーバーに，リモートデスクトップでログオンする」という。）（甲１８の４）。

ｂ　Ａは，本件リモートメンテナンスサーバーから，さらに，リモートデスクトップで他のサーバーにログオンした。Ａは，本件顧客データベースサーバーの中に，最新の顧客データベースのバックアップファイルを見つけ，ファイル圧縮ソフトを使用して，同ファイルの圧縮作業を開始したが，圧縮作業に時間が掛かることから，その状態で，被告ＢＢテクノロジーのサーバーへの接続を切断した（甲１８の４，１８の６）。

（イ）　６月２７日のアクセス

ａ　６月２７日，Ａは，Ｂと共に，インターネットカフェに行き，店内のパソコンから，本件アカウントを用いて，本件リモートメンテナンスサーバーにリモートデスクトップで接続した（甲１８の４，１８の６）。

ｂ　Ａは，さらに，（ア）ｂの圧縮作業を行ったサーバーにリモートデス

クトップでログオンし，圧縮結果を確認した上で，同ファイルを，被告ＢＢテクノロジーのサーバーから，店内のパソコンに接続した外付けハードディスクに転送する作業を開始した。

この外付けハードディスクは，Ｂが用意したもので，Ａらが，インターネットカフェに持ち込み，店内のパソコンに接続していたものであった（以下，このハードディスクを「本件外付けハードディスク」という。）（甲１８の４，１８の６）。

ｃ　ファイルの容量が大きく，ファイル転送に約２日かかる計算であったため，Ｂが店員に交渉して，Ａらが使用しているパソコンを誰も使えないようにしてもらった上で，Ａらは店を出た（甲１８の４，１８の６）。

（ウ）　６月３０日の顧客情報の取得

Ａの仕事の都合があったため，Ｂは，６月３０日，(イ)のアクセスの際と同じインターネットカフェに一人で赴き，(イ)ｂの転送の結果を確認したところ，ファイルの転送は完了しており，店内のパソコンに接続していた本件外付けハードディスクを取り外して，自宅へ持ち帰った（以下，この際にＢが取得したデータを「６月のデータ」という。）（甲２０の２１）。

ウ　Ｂは，６月１３日のアクセス以前は，本件リモートメンテナンスサーバーを通じて，被告ＢＢテクノロジーのサーバーにアクセスする方法を知らなかった。しかし，同月１３日，２０日，２７日のアクセスの際に，Ａがパソコンを操作するのを見たり，Ａからの説明を受けたことを通じて，

・本件リモートメンテナンスサーバーのＩＰアドレス

・本件アカウントや本件データベースアカウント

・本件アカウントが，リモートメンテナンスサーバー以外のサーバーにも設定されていること

・本件リモートメンテナンスサーバーに登録されているユーザー名の中に，ユーザー名とパスワードが同じものが多数存在すること。

・本件顧客データベースサーバーや，本件バックアップサーバーの存在等を知ったものである。

エ　なお，Ａは，６月２０日のアクセスの際に，６月のデータ以外に，被告ＢＢテクノロジーのサーバー内の幾つかのファイルを本件外付けハードディスクに転送して入手した。また，その際に，旧バックアップサーバーから，本件顧客データベースの古いバックアップファイルの取得を試みたが，Ａが旧バックアップサーバーから転送したバックアップファイルは，後日確認した結果，データの圧縮・転送に失敗しており，復元ができないことが確認された（甲１８の４，２０の３，２０の２１）。

(3)　Ｂによる６月のデータの復元と独占

ア　Ｂは，６月のデータの取得後，これの転送が完了した旨をＡに報告したが，両名は，すぐに顧客情報を処分すれば，被告ＢＢテクノロジーが不正アクセスに気付くのではないかと考え，しばらくの間，同ファイルをそのままに置いておくことにした。そのため，Ｂが回収した本件外付けハードディスクは，そのままＢが保管することとなった（甲１８の４，２０の２１）。

イ　Ｂは，平成１５年９月中旬ころ，自己のパソコンを用いて，６月のデータの復元を試みたところ，復元に成功し，６月のデータには，４７１万６７８８人分の個人情報が含まれていることを確認した。

当初，ＡとＢの間では，被告ＢＢテクノロジーから取得した顧客情報を第三者へ処分し，その利益を分配する予定であったが，Ｂは６月のデータを独り占めしようと考えた（甲２０の４，２０の６，２０の１７，２０の２１）。

ウ　同年１０月ころ，Ａが，Ｂに連絡し，６月のデータの復元作業を行うこ

ととなったが，Ｂは，既に復元に成功したことをＡに告げず，さらに顧客データベースの一部を故意に破損させ復元が不可能となったデータベースファイルをＡに手渡し，Ａに本件顧客データベースサーバーからの転送が失敗したと誤信させた（甲１８の４，２０の２１）。

(4)　ＢとＥの接触

Ｂは，平成１５年１０月初めころ，知人の紹介で，右翼団体関係者であるＤの娘婿であるＥと会い，Ｅに６月のデータの売却等の処分先の仲介を依頼した（甲１９の２，２０の１７）。

Ｂは，６月のデータの一部を印刷し，Ｅに渡したが，見づらいものであったため，６月のデータを，データの項目を絞り込んだ上で，マイクロソフト社のデータベースソフトであるアクセスを用いて見やすい表にして印刷し，同年１１月下旬ころに，再度Ｅに渡した。Ｄは，６月のデータの処分の話をＥから聞いており，それらの資料は，ＥからＤへと渡った（甲１９の３～４，１９の１０，２０の６～７，２０の１７，２４の７）。

(5)　Ａによる再度のアクセスとＢによる本件アカウントの消去等

ア　本件顧客データベースのデータの取得に失敗したと信じていたＡは，平成１５年１１月中旬ころから，Ｂに対し，なおも本件顧客データベースのデータの取得を持ちかけてくるようになり，Ｂはこれに応じることにした。両者は，同年１２月２９日に再度，被告ＢＢテクノロジーのサーバーにアクセスを試みることにした（甲１８の５，２０の２１）。

イ　Ｂは，同年１１月２４日，インターネットカフェのパソコンから，本件アカウントを用いて，本件リモートメンテナンスサーバーにリモートデスクトップでログオンし，本件アカウント等が変更されていないことを確認した（甲２０の２１）。

ウ　１２月２７日の本件アカウントの消去

Ｂは，Ａによる顧客情報の取得を妨害するため，同年１２月２７日，イ

ンターネットカフェ内のパソコンから，本件アカウントを用いて，本件リモートメンテナンスサーバーにリモートデスクトップでログオンした。Ｂは，ログオン後，本件リモートメンテナンスサーバーから，本件アカウントを消去した（甲２０の２１）。

エ　１２月２９日のＡとＢのアクセス

同月２９日，ＡとＢは，インターネットカフェに行った。Ａは，店内のパソコンから，本件アカウントを用いて，リモートデスクトップで本件リモートメンテナンスサーバーにログオンしようとしたが，ログオンすることができなかった。そのためＡは，知っている別のユーザー名とパスワードを入力し，本件リモートメンテナンスサーバーにリモートデスクトップでログオンすることに成功した。

Ａは，本件顧客データベースサーバー内の最新のバックアップファイルを圧縮する作業を開始した上，被告ＢＢテクノロジーのサーバーとの接続を切り，ＡとＢはインターネットカフェから出た（甲１８の５，２０の２１）。

オ　Ｂによる圧縮作業の中断と，パスワード変更

（ア）　Ｂは，Ａが新たに顧客情報のデータを取得すれば，既に自らが保有しているデータの価値が下がってしまうと考え，１２月２９日，Ａと別れた後に再度インターネットカフェに行った。そして，店内のパソコンから，本件アカウントを消去する際にユーザー名の一覧で見て記憶していた別のユーザー名（このユーザー名は，ユーザー名とパスワードが同一であった。）を用いて，本件リモートメンテナンスサーバーにリモートデスクトップでログオンし，Ａの行った圧縮作業を中断した（甲２０の２１）。

（イ）　Ｂは，同日，さらに，本件リモートメンテナンスサーバーに登録されているユーザー名のうち，Ａが知っていると思われる複数のユーザー

名のパスワードを変更し，Ａのデータ取得を妨害した（甲２０の２１，２０の２５）。

（ウ）　Ｂは，１２月３１日にも，インターネットカフェのパソコンから，同様に，本件リモートメンテナンスサーバーに登録されているユーザー名のうち，ユーザー名とパスワードが同じものについて，パスワードを変更した（甲２０の２２，２０の２５）。

（エ）　１２月２９日と３１日の作業の際には，Ｂは，本件監視サーバーにも，本件アカウントを用いて，リモートデスクトップでログインした上で，登録されているユーザー名を確認し，そのパスワードを変更した（甲２０の２５）。

(6)　ＢとＤの接触

Ｂは，１２月３１日，Ｅに誘われて，Ｄの忘年会に出席し，その際に，Ｄに初めて会った。Ｂは，Ｄによる被告ＢＢテクノロジー等を恐喝する計画について，それまで聞かされていなかった。

翌日の平成１６年1月１日に，Ｄは，ＢとＥに，被告ＢＢテクノロジー等を恐喝する計画であることを告げ，Ｂに，被告ＢＢテクノロジー内に存在する新たなデータや6月のデータよりも重要なデータを取得すること，被告ＢＢテクノロジーのサーバーに侵入したのが中国人であるように見せかけることなどを指示した（甲１９の7，１９の１０，２０の１８，２４の8）。

(7)　被告ＢＢテクノロジーのパスワード変更等への対処

ア　Ｂが，(5)オ(イ)のとおり，本件リモートメンテナンスサーバーに登録されていたユーザー名のパスワード変更を行ったため，平成１５年１２月３０日，被告ＢＢテクノロジーの従業員が，本件リモートメンテナンスサーバーへログオンできない事態が生じた（甲１１の４，１３の１）。

Ｆは，本件リモートメンテナンスサーバーと，本件監視サーバーに登録されていたパスワードが変更されていることに気付き，その旨の社内メー

ルを送信して注意を喚起した。また，Ｆは，パスワードが書き換えられてログオンできなかったユーザー名については，書換え前のものにパスワードの再設定を行った（甲１１の４）。

イ　また，平成１６年１月５日，本件リモートメンテナンスサーバーに，被告ＢＢテクノロジーの従業員がログオンできない事態が生じた。その際の調査で，本件リモートメンテナンスサーバーについて，本件アカウントが削除されていること，アで再設定したパスワードが再び書き換えられていることが確認された（甲１１の４，１３の１）。

(8)　１月の不正取得

ア　Ｂによるパスワード変更の有無の確認

Ｂは，平成１６年１月１日及び８日，(5)のパスワード変更等に，被告ＢＢテクノロジーが気付いて対応しているかを確認するため，インターネットカフェのパソコンから，自分がパスワードを変更したユーザー名を用いて，変更後のパスワードを入力して，本件リモートメンテナンスサーバーにログオンを試みた（甲２０の２２）。

同月１日には，変更後のパスワードでログオンできたが，８日には，変更後のパスワードで，ログオンすることができず，Ｂは，被告ＢＢテクノロジーがパスワードの変更に気付いたことが分かった。Ｂは，８日のアクセスの際に，念のため，変更前のパスワードでログオンすることを試み，変更前のパスワードでログオンが可能であり，一部のユーザー名のパスワードがＢによって変更される以前のものに戻されていただけであることを確認し，Ｂは再度パスワードを変更した（甲２０の２２，２０の２５）。

イ　中国人のアクセスに見せかけるための工作

１月１０日，Ｂは，インターネットカフェ内のパソコンから，本件リモートメンテナンスサーバーにリモートデスクトップでログオンし，本件リモートメンテナンスサーバー内に，中国人の犯行に見せかけるための英文

のテキストファイルを作成・保存した（甲２０の１０，２０の２５）。

ウ　１月１３日のアクセス

（ア）　本件顧客データベースからのデータの抽出・圧縮

１月１３日，Ｂは，インターネットカフェのパソコンから，本件リモートメンテナンスサーバーに，リモートデスクトップでログオンし，さらに本件顧客データベースサーバーにリモートデスクトップでログオンした。本件顧客データベースサーバーにログオンする際には，Ｂは，本件アカウントではなく，本件データベースアカウントを使用した。

Ｂは，本件顧客データベースサーバー内にあったデータベースを操作するソフトを用いて，本件顧客データベースの中から，顧客情報を抽出する作業を行い，抽出したデータを圧縮した（甲２０の２２，２０の２７）。

（イ）　圧縮後のデータの転送

同日，Ｂは，(ア)とは別のインターネットカフェに行き，本件リモートメンテナンスサーバーにリモートデスクトップで接続し，本件顧客データベースサーバーとは別のサーバーに(ア)の圧縮したデータをコピーした上で，同サーバーに本件アカウントでリモートデスクトップで接続し，そのサーバーから，(ア)の圧縮したデータを，店内のパソコンに接続した外付けハードディスクに転送した（以下，この際にＢが取得したデータを「１月のデータ」という。）。

１月のデータには，約６５０万件の顧客情報が含まれていた。

この外付けハードディスクは，本件外付けハードディスクとは別のハードディスクで，Ｂが，自宅のパソコンで６月のデータの復元作業に使用していたものを取りだして，外付け用のケースに入れたものであった（甲２０の１３，２０の２２，２０の２７）。

（ウ）　同日のアクセスの際に，Ｂは，本件顧客データベースサーバー内に，

被告ＢＢテクノロジーが提供するＩＰ電話サービス「ＢＢフォン」の通話記録データの一部を発見し，１月のデータと同様に，このデータも抽出・圧縮した上で，被告ＢＢテクノロジーのサーバーから，インターネットカフェのパソコンに接続した外付けハードディスクに転送した（甲１５，１６，２０の２２，２０の２７）。

エ　なお，同月１１日，１２日にも，Ｂは，本件リモートメンテナンスサーバーにリモートデスクトップでログオンしており，被告ＢＢテクノロジーからデータを転送するためのテスト等を行い，１２日には，１３日と同様の方法で，顧客データの転送を試みたが，何らかの原因で転送が失敗したものであった（甲２０の２２，２０の２６，２０の２７）。

(9)　ＤＶＤ－Ｒ等の作成・Ｄらによる入手

ア　１月２１日ころ，Ｄは，Ｅを通じて，Ｂに対し，取得した顧客情報のデータそのものを引き渡すように指示した（甲１９の６，２４の１１）。

イ　ＢはＤの指示を受けて，同月２２日に，１月のデータをアクセスで加工した上で，ＣＤ－Ｒに１０万人分，ＤＶＤ－Ｒに４５０万人分の顧客情報を記録し（以下，それぞれ「本件ＣＤ」「本件ＤＶＤ」という。），同月２３日，これらをＤに渡した（甲２０の１２，２０の１９，２０の２２，２０の２７）。

ウ　なお，Ｂは，同月，６月のデータの一部を抽出して印刷したものや，(8)ウ(ウ)の通話記録の一部を印刷したものも，ＥないしＤに渡している（甲１９の５，２０の１１～１２，２０の１４，２０の２７，２４の１２）。

エ　１月２３日，Ｄは，本件ＣＤ及び本件ＤＶＤを，本件恐喝未遂事件の実行犯であるＣに渡した（甲２４の５，２４の１２）。

(10)　Ａ・Ｂらによる顧客情報等の処分

ア　Ａは，平成１６年１月３日，インターネットカフェのパソコンから本件

リモートメンテナンスサーバーへリモートデスクトップでログオンしようとしたがログオンできず，不正アクセスが被告ＢＢテクノロジーに発覚していると思ったため，被告ＢＢテクノロジーから入手したデータの入っていたハードディスクは破棄し，Ｂから預かっていた本件外付けハードディスクは，動画データを何度も上書きして，元のデータが復元できないようにした（甲１８の５～６）。本件外付けハードディスクはその後，Ａの自宅から押収された（甲１８の４，２０の２４）。

イ　Ｂは，同月２３日，本件ＤＶＤ及び本件ＣＤを渡した後に，被告ＢＢテクノロジーの顧客情報を保存していたハードディスクを電子レンジにかけて，中のデータを破壊し，そのハードディスクを捨てた（甲２０の１５，２０の１９）。

ウ　本件ＣＤ及び本件ＤＶＤは，同月２３日，Ｃから被告ＢＢテクノロジーに渡り，その後，同被告から警察に提出されて，警察が領置した（甲１０の２，２０の１２，２４の５）。

２　被告ＢＢテクノロジーの過失について

(1)　注意義務の内容

ア　個人情報の管理に関する一般的な注意義務

本件サービスが電気通信事業法上の電気通信事業に当たることは争いがなく，被告ＢＢテクノロジーは同法にいう電気通信事業者に当たると認められる（乙３）ところ，本件不正取得が行われた当時，電気通信事業における個人情報保護に関するガイドライン（平成１０年１２月２日郵政省告示５７０号）５条４項は，「電気通信事業者が個人情報を管理するに当たっては，当該情報への不正なアクセス又は当該情報の紛失，破壊，改ざん，漏えいの防止その他の個人情報の適切な管理のために必要な措置を講ずるものとする。」と定めていた。

また，被告ＢＢテクノロジーは，第２の１(3)ア，(4)のとおり，原告ら

を含む本件サービスの顧客の個人情報をデータベースとして保有，管理しており，個人情報保護法にいう個人情報取扱事業者に当たると解されるところ，同法２０条は，「個人情報取扱事業者は，その取り扱う個人データの漏えい，滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。」と定めている（なお，同法は，平成１５年５月３０日に成立したが，本件不正取得が行われた当時は，まだ施行されていなかった。）。

これらの点に鑑みると，被告ＢＢテクノロジーは，本件不正取得が行われた当時，顧客の個人情報を保有，管理する電気通信事業者として，当該情報への不正なアクセスや当該情報の漏えいの防止その他の個人情報の適切な管理のために必要な措置を講ずべき注意義務を負っていたと認められる。

イ　リモートアクセスに関する注意義務

上記のとおり，本件においては，本件リモートメンテナンスサーバーを通じて，本件顧客データベースサーバーにリモートアクセスが可能な状態となっていた。

リモートアクセスについては，ＪＩＳ規格や，コンピュータ不正アクセス対策基準（平成８年通商産業省告示第３６２号）で，その危険性が指摘され，不正アクセスへの対策について各種の規定がされているところであり（規定の内容については被告らも争わない。），これらの規定等の存在が示すように，あるサーバーに対してリモートアクセスを可能にすることは，それ自体，当該サーバーに対する外部からの不正アクセスの危険を高めるものであるといえる。

被告ＢＢテクノロジーは，個人情報の管理に関してアのとおりの注意義務を負うのであるから，本件顧客データベースサーバーについて，そもそも必要性がない場合又は必要性のない範囲にリモートアクセスを認めるこ

とは許されず，また，リモートアクセスを可能にするに当たっては，不正アクセスを防止するための相当な措置を講ずべき注意義務を負っていたというべきである。

(2)　リモートアクセスに関する注意義務違反の存否

ア　リモートアクセスの必要性及びその範囲の相当性

(ア)　被告ＢＢテクノロジーが，平成１４年１２月に本件リモートメンテナンスサーバーを設置して，本件顧客データベースサーバーへのリモートアクセスを可能にしたのは，前記のとおり，休日や夜間に社外からサーバーのメンテナンスを行う必要からというものであった。

乙６の１によれば，同年１２月当時の本件サービスの利用状況については，同月末の接続回線数が約１６９万件であり，前月に比べ約２３万件の増加をしていたと認められ，同月当時，新規加入の顧客情報の入力や，登録された情報の変更等の作業は相当な量に上るものと推認でき，顧客データベースに不具合が生じた場合に至急復旧する必要性もあったと認められる。また，本件顧客データベースサーバーについて，前記のとおり，同年１１月に実際にトラブルが生じていることにも照らせば，同年１２月当時，被告ＢＢテクノロジーにおいて，社外からメンテナンスを行うため，リモートアクセスを認める必要性がなかったとはいえない。

(イ)　また，本件アカウントに，本件リモートメンテナンスサーバーや，本件顧客データベースサーバーを含むその他のサーバーについての管理者権限を与えていたことについても，前記のとおり，社外からのメンテナンス作業を行うためにこれを付与していたと認められるから，メンテナンス作業に必要な範囲を超えた権限を与えていたとはいえない。

イ　不正アクセス防止のための相当な措置

(ア)　アクセス管理の体制

前記のとおり（第２の１(6)ウ），本件リモートメンテナンスサーバーについては，そのＩＰアドレスを特定して，登録されたユーザー名・パスワードを入力すれば，リモートデスクトップでログオンすることが可能であって，被告ＢＢテクノロジーは，本件リモートメンテナンスサーバーに対するアクセス管理として，ユーザー名とパスワードによる認証を行っていたが，特定のコンピュータ以外からはリモートアクセスができないようにする措置はとられていなかったものと認められる。

なお，証拠（甲２５，２６，乙７の１６）及び弁論の全趣旨によれば，本件不正取得当時において，リモートアクセスを認める場合に，ユーザー名とパスワードによる認証以外に，コールバック機能等を使用することによって，特定のコンピュータからのアクセスしか認めないというようなアクセス規制をする方法は存在したものと認められる。

（イ） ユーザー名とパスワードの管理

本件においては，前記のとおり，本件リモートメンテナンスサーバーに登録されているユーザー名とパスワードについて，被告ＢＢテクノロジーは，①本件アカウントを共有アカウントとしてＡに与えていたこと，②平成１５年２月末にＡが退職した際に，本件アカウントを含めＡが知り得たユーザー名を削除したりそのパスワードを変更したりしなかったこと，③本件リモートメンテナンスサーバーの設置から平成１６年１月までの約１年間，登録されているユーザー名について，パスワードの定期的な変更を行わなかったことが認められる。

また，前記のとおり，④平成１５年１２月３０日と平成１６年１月５日に，本件リモートメンテナンスサーバーに登録されていたユーザー名のパスワードが変更されていたり，本件アカウントが削除されていたりしたことに気付いていたものの，パスワードが変更されていたユーザー名について元のパスワードに戻して，その使用を継続させていた。

（ウ） 以上の被告ＢＢテクノロジーにおけるリモートアクセスの管理体制は，ユーザー名とパスワードによる認証以外に外部からのアクセスを規制する措置がとられていない上，肝心のユーザー名及びパスワードの管理が極めて不十分であったといわざるを得ず，同被告は，多数の顧客に関する個人情報を保管する電気通信事業者として，不正アクセスを防止するための前記注意義務に違反したものと認められる。

なお，同被告は，本件リモートメンテナンスサーバーのＩＰアドレスを第三者が特定することは困難であると主張する。しかし，同被告は，退職した元従業員等，もともと本件リモートメンテナンスサーバーのＩＰアドレスを知り得る立場にある者による不正アクセスについても，これを防止するための相当な措置を講ずべきであると解されるから，ＩＰアドレスの特定の困難性は上記判断に影響を与えるものではない。

(3) 予見可能性及び結果回避可能性について

ア 予見可能性

前記のとおり，Ａは，被告ＢＢテクノロジーにおいて，本件顧客データベースサーバーを含むサーバー管理業務を行っており，又，リモートアクセスを業務上認められていた。また，乙１０によれば，被告ＢＢテクノロジーは，Ａが被告ＢＢテクノロジーでの業務を始めるに当たって，被告ＢＢテクノロジーの営業上ないし技術上の情報についての秘密保持等に関する誓約書を書かせていたことが認められる。

被告ＢＢテクノロジーがＡに行わせていた業務の内容，与えていた権限の内容に，前記誓約書を書かせていたことを総合すれば，Ａが業務を終える際に同被告とトラブルがあったか否かにかかわらず，同被告は，Ａが業務を終えた後に，業務中に知り得たパスワード等の情報を用いたり，他人にそれらの情報を漏らしたりすることによる不正アクセスについては，予見可能であったというべきであり，本件不正取得についても予見可能であ

ったと認められる。

イ　結果回避可能性

本件において，後記のとおり原告らの個人情報が含まれていたと認められるのは１月のデータであるが，Ｂによる１月のデータの不正取得については，それまでに，被告ＢＢテクノロジーが，本件アカウントを含むユーザー名・パスワードの適切な管理等，不正アクセスを防止するための相当な措置を採っていれば防ぎ得たといえるから，結果回避可能性も認められる。

この点，被告ＢＢテクノロジーは，Ａはその他のパスワード等によって被告ＢＢテクノロジーのサーバーに侵入することも可能であった等として，本件アカウントについて，いくら厳重に管理していても，Ｂによる１月のデータの取得は防止できなかったと主張する。

確かに，前記本件不正取得の経緯のとおり，Ｂは，平成１５年１２月２７日，本件リモートメンテナンスサーバーから，本件アカウントを削除しており，その後は，本件リモートメンテナンスサーバーにリモートデスクトップでログオンする際には，自らがパスワードを変更したユーザー名を用いるなどして，本件アカウントを使用していない。

しかし，本件リモートメンテナンスサーバーに多数のユーザー名・パスワードを登録している状況において，不正アクセスを防止するための相当な措置をとるためには，本件アカウントを含め，それら全体について適切な管理を行うべきことは当然である。１月のデータの不正取得については，前記の本件不正取得の経緯に照らし，例えば，本件アカウントのみならず，サーバー管理業務を行っていたＡが知り得たと思われるユーザー名について，Ａの退職時にこれを削除したり，パスワードを変更することによって防げた可能性が高いし，パスワードについての定期的な変更を行ったり，又は，平成１６年１月に第三者によってパスワードが変更されていること

に気付いた際など，全面的なパスワード変更を少なくとも１回行うことによっても防ぎ得たといえるから，この点についての被告ＢＢテクノロジーの主張は採用できない。

(4)　以上によれば，被告ＢＢテクノロジーは，本件リモートメンテナンスサーバーを設置して本件顧客データベースサーバー等のサーバーへのリモートアクセスを行うことを可能にするに当たり，外部からの不正アクセスを防止するための相当な措置を講ずべき注意義務を怠った過失があり，同過失により本件不正取得を防ぐことができず，原告らの個人情報が第三者により不正に取得されるに至ったというべきである。したがって，同被告は，原告らに対し，本件不正取得により原告らの被った損害を賠償すべき不法行為責任がある。

３　被告ヤフーの過失及び共同不法行為責任について

(1)　自己の保管する個人情報に対する管理義務違反

証拠（甲１０の１，２１の１，乙３）及び弁論の全趣旨によれば，被告ヤフーと被告ＢＢテクノロジーは，その管理している情報の範囲も異なり（被告ヤフーのみが利用料の徴収業務を行い，クレジットカード番号等の決済情報を保有していた。），顧客情報をそれぞれ別個に管理していたものと認められ，本件全証拠によっても，被告ヤフーが管理していた顧客情報が流出したとは認められない。

したがって，被告ヤフーが自らの管理していた顧客情報に対する管理義務に違反し，同被告の管理する原告らの個人情報が漏えいしたとの事実は認められず，この点に関する原告らの主張は理由がない。

(2)　被告ＢＢテクノロジーに対する監督義務違反等

ア　監督義務違反等による過失の有無について

証拠（甲１０の１，乙３）及び弁論の全趣旨によれば，被告らは，原告らを含む顧客と，それぞれ別個の契約を締結し，それぞれが顧客から個人

情報の提供を受け，別個のサービスを提供していたものと認められ，また，前記のとおり，その管理している情報の範囲も異なり，別個のサーバーに保管管理していたものである。

確かに，証拠（甲１０の１，２１の１，乙１の２，２～４）及び弁論の全趣旨によれば，原告らの主張するように，被告らは，共に株式会社ソフトバンクの子会社であり，本件サービスの契約手続などにおいて外形上一体のものとして本件サービスを提供していたものであり，また，利用料の徴収のため，被告ＢＢテクノロジーは，回線使用料のデータ等を被告ヤフーに送っていたこと，申込者のデータの入力の作業の際に，申込時に提供された個人情報が被告ヤフーを通じて被告ＢＢテクノロジーに送られていたことが認められる。

しかし，これらの事情を総合したとしても，本件において，被告ヤフーが，被告ＢＢテクノロジーが別個に保管していた顧客情報について，適切に管理すべき義務を負っていたとは認められない。また，同様に，被告ヤフーが，被告ＢＢテクノロジーが顧客情報を適切に管理するよう監督すべき義務を負っていたともいえない。

以上のとおりであって，被告ＢＢテクノロジーの管理する情報が不正取得されたことについて，被告ヤフーの過失は認められない。

イ　したがって，その余の点について判断するまでもまく，上記過失を前提として，被告ヤフーが被告ＢＢテクノロジーと共同不法行為責任を負うとの主張には理由がない。

４　原告らの権利侵害について

(1)　不正取得された原告らの個人情報

前記のとおり，Ｃが取得した顧客データは，１月のデータの一部を本件ＤＶＤ及び本件ＣＤに記録したものと認められ，その中に，原告らの個人情報が含まれていたことは争いがないから，１月のデータに原告らの個人情報が

含まれていたことが認められる。

Ａ及びＢは，前記のとおり，１月のデータの他にも，６月のデータや通話記録等を被告ＢＢテクノロジーのサーバーから不正に取得しているが，本件全証拠によっても，これらに，原告らの個人情報が含まれていたとは認められない。

(2)　１月のデータの流通範囲（二次流出の有無）

１月のデータは，前記のとおり，Ｂが取得し，本件ＤＶＤ及び本件ＣＤに記録され，Ｄを通じてＣに渡り，Ｃから被告ＢＢテクノロジーに渡ったことが認められる。また，１月のデータの処分については，前記のとおり，これが入ったハードディスクはＢにより，電子レンジにかけて破壊された上で破棄されていること，本件ＤＶＤ及び本件ＣＤは押収されていることが認められる。

原告らは，この点，本件ＤＶＤ及び本件ＣＤをＣらが複製した可能性がある旨主張する。しかし，証拠（甲１０の２，２４の５，２４の１２）及び弁論の全趣旨によれば，Ｃが本件ＤＶＤ及び本件ＣＤを取得したのは，被告ＢＢテクノロジー側と接触する直前であり，Ｃは，その日の接触の際にこれらを被告ＢＢテクノロジー側に渡しているのであって，複製作業等を行う時間的余裕があったとは考えがたく，本件全証拠に照らしても，このような複製の事実を認めることはできない。

また，インターネットやマスコミに流出したデータについては，本件全証拠に照らしても，１月のデータであるとは認められず，また，それらの中に原告らのデータが含まれているとも認められない。

以上のとおりであり，本件において，１月のデータが，Ｂ及びＣら本件恐喝未遂関係者からさらに他の者に流出（以下，「二次流出」という。）したとは認められない。

(3)　権利侵害

ア　上記のとおり，Ｂ，Ｃらが取得した１月のデータは原告らそれぞれの個人情報を含み，その内容は，①住所②氏名③電話番号④メールアドレス⑤ヤフーＩＤ⑥ヤフーメールアドレス⑦申込日を含むものであった。

イ　上記①～⑥の住所・氏名・電話番号・メールアドレス等の情報は，個人の識別等を行うための基礎的な情報であって，その限りにおいては，秘匿されるべき必要性が高いものではない。また，本件サービスの会員であるということ及びその申込日についても同様である。

しかし，このような個人情報についても，本人が，自己が欲しない他者にはみだりにこれを開示されたくないと考えることは自然なことであり，そのことへの期待は保護されるべきものであるから，これらの個人情報は，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というべきである。

ウ　被告らは，本件において二次流出は確認できず，原告らの個人情報が文字としてモニターに表示されたり印刷されたりして外部から認識可能な状態で開示されたことがない等として，原告らの権利は侵害されていないと主張する。

しかし，１月のデータは，前記のように，Ｂによって不正に取得され，Ｂがアクセスを用いて加工し，原告らの個人情報を含むその一部を記録した本件ＤＶＤ及び本件ＣＤがＤ及びＣに渡っているのであって，二次流出が認められなくても，これらのこと自体によって原告らのプライバシーの権利は侵害されたものといえる。

５　損害について

(1)　前記のとおり，被告ＢＢテクノロジーの過失により，１月のデータが不正取得され，原告らのプライバシーの権利が侵害されたというべきであるから，被告ＢＢテクノロジーは，これによって原告らが被った精神的苦痛について，原告らに対して，損害賠償責任を負うものである。

(2)　原告らは，損害の内容として，不正取得された原告らの個人情報が不特定の第三者にいついかなる目的でそれが利用されるか分からないという不安感を主張する。

確かに，本件においては，原告らの個人情報は，Ｄらの手に渡り，恐喝未遂という犯罪に用いられたものであり，それらの者が，自己の利益を図るために，恐喝以外の手段に原告らの個人情報を利用した危険性はあったものと考えられる。

しかし，１月のデータの回収状況については，４(2)のとおり，二次流出があったとは認められない状況であり，その意味で，１月のデータの流出についての原告らの不安感は，さほど大きいものとは認められない。

(3)　これらの事情のほか，１月のデータに含まれていた原告らの個人情報は秘匿されるべき必要性が必ずしも高いものではなかったこと，被告ＢＢテクノロジーが，本件恐喝未遂事件後，顧客情報の社外流出について発表を行い，不正取得されたことが確認できた顧客に対してその旨連絡するとともに，本件サービスの全会員に５００円の金券を交付するなどして謝罪を行う一方，顧客情報についてのセキュリティ強化等の対策をとっていること（乙７の１～１６，弁論の全趣旨）といった本件に現れた一切の事情を考慮すると，原告らの精神的苦痛に対する慰謝料としては一人あたり５０００円と認めるのが相当である。

弁論の全趣旨によれば，原告らは，甲・乙事件訴訟代理人弁護士らに本件訴訟の提起・追行を委任しており，これに対する報酬の支払を約したと認められ，被告ＢＢテクノロジーの不法行為と相当因果関係のある弁護士費用は一人あたり１０００円と認めるのが相当である。

６　結論

よって，原告らの本訴請求は，被告ＢＢテクノロジーに対し，それぞれ６０００円及びこれに対する甲事件原告らについては平成１６年５月２９日から，

乙事件原告らについては平成１７年６月３日からそれぞれ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理由があるから認容し，同被告に対するその余の請求及び被告ヤフーに対する請求は理由がないからこれを棄却し，訴訟費用の負担につき民事訴訟法６１条，６４条本文，６５条１項本文を，仮執行宣言につき同法２５９条１項をそれぞれ適用して，主文のとおり判決する。

大阪地方裁判所第１１民事部

裁判長裁判官　　山　　下　　郁　　夫

裁判官　　横　　路　　朋　　生

裁判官　　矢　　野　　紀　　夫