2014 年 9 月 25 日

各　　位

会 社 名：株式会社ベネッセホールディングス
代表者名：代表取締役会長兼社長　原田　泳幸
（コード番号：9783　東証第一部）
会 社 名：株式会社ベネッセコーポレーション
代表者名：代表取締役社長　　小林　仁

問合せ先：株式会社ベネッセホールディングス
ブランド・広報部長　　小沼　和幸
（TEL：03－5320－3503）

個人情報漏えい事故調査委員会による調査結果のお知らせ

株式会社ベネッセホールディングス（以下、弊社）は、株式会社ベネッセコーポレーションのお客様情報の漏えいに関して、本年 7 月 15 日に小林英明弁護士を委員長とする「個人情報漏えい事故調査委員会」を設置し、外部の専門家と共に徹底した事実調査・原因究明および再発防止策の策定に取り組んでまいりました。

調査結果につきましては、9 月 12 日付で、弊社代表取締役会長兼社長 原田泳幸が、同委員会より最終報告書を受領いたしました。

「調査報告（公表版）」につきましては、別紙をご覧ください。

弊社は、本調査結果を真摯に受けとめ、お客様はもちろん関係各位に、多大なご迷惑をお掛けし、ご心配をいただきましたことを、改めまして深くお詫び申し上げます。今後二度とこのような事態を起こすことのないよう、早急に再発防止策を実行し、全力でお客様の信頼回復に取り組んでまいります。

以　　上

平成 26 年 9 月 25 日

個人情報漏えい事故調査委員会による調査報告について

株式会社ベネッセホールディングス

弊社は、弊社の完全子会社である株式会社ベネッセコーポレーション（以下「**BC**」という。）において、平成 26 年 7 月に発覚した個人情報漏えい事故に関し、同年 9 月 12 日に、個人情報漏えい事故調査委員会（以下「**本調査委員会**」という。）から調査報告を受けましたので、その概要を、以下のとおりご報告いたします[1]。

第１章　序

Ⅰ．調査に至る経緯

平成 26 年 6 月 27 日、BC は、顧客からの問い合わせにより、BC の顧客の情報が社外に漏えいしている可能性を認識した。そこで、BC の代表取締役社長小林仁の指揮のもと、BC は、緊急対策本部を設置するとともに、これらの問い合わせで提供された情報を手がかりとして社内調査を開始した。この調査により、同年 7 月 7 日、BC からの漏えい情報であることが確認されたため、株式会社ベネッセホールディングス（以下「**BHD**」という。）代表取締役会長兼社長・原田泳幸（以下「**原田会長兼社長**」という。）の指揮のもと、緊急対策の意思決定機関として危機管理本部を設置し、外部の情報セキュリティ専門家等を招聘し、データベースの安全確保のための緊急対策を講じ、顧客情報の拡散防止の活動を開始した。

社内調査の結果、BC の顧客及び BC が契約によらずに個人情報を取得した者[2]（以下「**顧客等**」という。）の個人情報が BC の管理するデータベース（以下「**本件データベース**」という。）から社外に不正に持ち出されていた事実（以下「**本件個人情報漏えい事実**」という。）が存在する可能性が高いことが判明したため、BC は、警察に対する相談を開始し、同年 7 月 15 日には、警視庁に対して、本件個人情報漏えい事実についての刑事告訴（以下「**本件刑事告訴**」という。）を行った。本件刑事告訴を受け、同月 17 日、警視庁は、不正競争防止法違反の容疑で、BC のシステム開発・運用を行っているグループ会社・株式会社シンフォーム（以下「**シンフォーム**」という。）の業務委託先の元社員である松崎正臣（以下「**松**

[1] 本調査委員会から、平成 26 年 9 月 12 日に、詳細な調査報告書の提出を受けた。同調査報告書の内容には、BHD（後に定義する）及び BC の情報セキュリティ・営業ノウハウ等の機密に係わるものが多く含まれていること、並びに本件個人情報漏えい事実（後に定義する）に関する公的機関の捜査等が本調査委員会による調査と併行して行われていること等から、公表に適さない事項が多く存在するため、本書は、弊社の責任において、同報告書の概要をまとめたものである。

[2] 個人情報は本人の同意を得た上で取得している。

崎」という。）を逮捕した。

平成 26 年 7 月 15 日、BHD の危機管理本部は、原田会長兼社長の諮問機関として、BHD 又は BC の関係者ではない外部の専門家である小林英明弁護士を委員長とする**本調査委員会**を設置することを決定し、同月 22 日には、本調査委員会の構成メンバーを決定した。本調査委員会は、本件個人情報漏えい事実が BHD 及び BC が今現に直面している企業危機事案であり、早期の緊急的再発防止策の実施が急務であることに鑑み、本件個人情報漏えい事実に関する事実、原因等の調査（以下「**本調査**」という。）を可及的速やかに行い、その結果について原田会長兼社長に報告するとともに、その結果を踏まえた、再発防止策等について提言を行うことを目的とすることとした。

Ⅱ. 調査主体

本調査委員会の委員構成は以下のとおりである。なお、本調査委員会は、上記Ⅰ.のとおり、企業危機に対応するための、原田会長兼社長の諮問機関としての調査委員会であり、平成 22 年 7 月 15 日付日本弁護士連合会策定の「企業等不祥事における第三者委員会ガイドライン（平成 22 年 12 月 17 日改訂)」に準拠した、いわゆる日弁連ガイドライン型第三者委員会ではない。

委員長	小林　英明	（長島・大野・常松法律事務所　弁護士）
委　員	西本　逸郎	（株式会社ラック　取締役兼専務執行役員 CTO）
同	梅野　晴一郎	（長島・大野・常松法律事務所　弁護士）
同	亦野　誠二	（長島・大野・常松法律事務所　弁護士）
同	福原　賢一	（株式会社ベネッセホールディングス　代表取締役副社長兼 CFO）

Ⅲ. 本調査の目的

本調査の目的は、以下のとおりである。なお、本件個人情報漏えい事実に係る BHD 及び BC 並びにその関係者の法的責任の評価･検討は、本調査の目的とはされていない。

- 個人情報漏えい事実に関する事実及び原因を調査する。
- 上記調査により判明した事実及びその原因等に即した再発防止策等について原田会長兼社長に対し、提言を行う。

Ⅳ. 調査結果の報告方法

本調査委員会は、本調査終了後、原田会長兼社長に対し、調査結果を記載した調査報告書を提出し、調査結果を報告する。但し、与えられた調査目的に鑑み、本調査により判明した原因等に即した再発防止策等については、口頭や書面等によって、随時の提言を行うことがある。

Ⅴ． 調査期間

本調査の期間は、平成 26 年 7 月 22 日から同年 9 月 12 日までである。

Ⅵ. 調査方法

延べ 63 名に及ぶ関係者に対する事情聴取を中心に、関係資料等の分析・検討、及び現場検証等の調査を行った。

第 2 章　調査結果

Ⅰ． 事故発生当時の情報セキュリティの状況

１． 本件データベースおよびシンフォームの執務室

個人情報を取り扱う業務を行う執務室[3]を含む施設の入館は、入館許可証の発行を受けた者又は臨時入館許可証の貸与を受けた者のみが入室でき、入退室管理規程に従い、入退出等が管理されていた。また、出入口付近には、監視カメラを設置していた。

２．クライアント PC のセキュリティ対策

(a) クライアント PC の利用場所の制限

シンフォームが業務委託先に貸与したクライアント PC は、ワイヤーロックにより施錠されており、常時持出しができないようにされていた。

(b) クライアント PC のセキュリティ対策

シンフォームは、従業員及び業務委託先（以下「**業務担当者**」という）が業務で使用するクライアント PC に関するセキュリティ対策として、社内規程上又は運用上、主なものとして、以下のセキュリティ対策を導入していた。

- 社内規程上、各システムユーザーに対し、認証 ID を割り当て、パスワードを設定し、そのパスワードは定期的に更新することが定められていた。業務で使用する本件データベースへのアクセスを許可されたパソコン（以下「**クライアント PC**」という）にはネットワーク接続設定、標準ソフトウェアの搭載が行われ、各部門は、システム管理部門の許可なく標準仕様を変更することはできないこととされていた。また、社内規程上、クライアント PC によるネットワークの使用状況・内容について、操作ログを記録することが定められていた。
- クライアント PC は、セキュリティ対策の運用上、ファイル共有ソフトなどの不要なソフトのインストールが制御され、また、外部オンラインストレージ等の不要な外部サービスについては、URL フィルタリングツールにより接続ができないようになっていた。

３． シンフォームにおける個人情報保護に関する教育

[3] 本調査委員会は本調査の対象としていないが、BHD として、本件データベースは、堅牢かつ安全なデータセンターに設置され、専用回線でシンフォームの事業所と接続されていたことを確認している。

シンフォームでは、社内規程上、従業員に対して定期的に適切な教育を実施することが定められていた。具体的には、企業倫理、情報セキュリティ、個人情報保護、内部者取引防止及びパソコン利用等について、定期的な教育を実施することが定められており、委託業務に従事する業務従事者に対しても、業務従事前に情報セキュリティ研修及びテストを行い、当該テストに合格した者にのみ、委託業務に従事させていた。また、業務従事者に対して、情報セキュリティ研修を毎年受講させていた。

Ⅱ. 本件個人情報漏えい事実における松崎による不正行為等

1. 不正行為

松崎は、シンフォームにおいて、本件データベース内に保管されていたBCの顧客等の個人情報を抽出の上、松崎が業務において使用していたクライアントPCに保存し、不正行為の準備を行った。

その上で、松崎は、クライアントPC内に保存した顧客等の個人情報を、USBケーブルを用いて松崎所有のスマートフォンに転送し、その内蔵メモリに保存する等の態様により、BCの顧客等の個人情報を不正に領得した。

警察の捜査により、その後、松崎は、不正に領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、それぞれ売却したことが判明している。

2. 漏えいした顧客等の個人情報の件数

(1) 延べ件数の算出

BCは、警察から、鑑定の目的で、松崎が上記名簿業者3社に対して売却したとされる顧客等の個人情報のデータの提供を受けた。BCが、当該データの分析を行ったところ、延べ約2億1,639万件[4]の顧客等の個人情報が記録されていた。

この約2億1,639万件という件数は、松崎の行った名簿業者への売却行為により漏えいした顧客等の個人情報の延べ件数の全てであると断定することはできない。しかし、上記データの内容等を詳細に分析した結果、松崎の売却行為により漏えいした顧客等の個人情報の延べ件数は、この約2億1,639万件という件数を大きくは超えない可能性が高い。

(2) 完全に一致した個人情報の除外

上記(1)において認定したのは延べ件数であり、全く同じ内容の個人情報が複数個含まれている場合には、その複数個分が、漏えいした個人情報の件数として複数回計上されている。そこで、延べ件数のうち、全く同じ内容の個人情報については、1件のみを計上した。

その結果、全く同じ内容の個人情報を除いた件数は、約6,984万件となった。

[4] 以下、千の位以下の件数及び人数は省略する。

(3)　名寄せ作業による重複の解消

上記(2)で認定した件数には、別個のデータとして存在していながらも、実際は同一人物のものと認められる個人情報が複数個存在しているが、これらについても、その複数個分が、漏えいした個人情報の件数として複数回計上されている。そこで、その重複を解消するために、名寄せ[5]の作業を実施した。

この名寄せの作業により、同一人物と認定されたものを 1 件として数えたところ、件数は約 3,504 万件、１件に複数の個人情報が登録されているケースもあり、人単位で数えると、個人情報が漏えいした者の人数は、約 4,858 万人となった。

Ⅲ.　不正行為等の原因（不正行為を防げなかったシステムの問題点）

1.　　不正行為等の原因となった情報処理システム

不正行為等の原因となった情報処理システムに関する問題点は、以下のとおりである。

(1)　アラートシステム

シンフォームにおいては、シンフォームの業務担当者が使用するクライアントPCから個人情報を保有するサーバへのアクセスについて、自動的にアクセスログ及び通信ログが記録されるように設定されていた。また、クライアントPCとサーバとの間の通信量が一定の閾値を超えた場合、データベースの管理者であるシンフォームの各担当部門の部長に対して、メールでアラートが送信される仕組み（以下、当該仕組みを「**本件アラートシステム**」という。）が採用されていた。しかし、本件アラートシステムの対象範囲が明確に定められていなかったことなどから、松崎による不正行為が行われた当時、クライアントPCと本件データベースとの通信を本件アラートシステムの対象として設定する措置が講じられておらず、松崎の不正行為等に対して本件アラートシステムが機能しなかった。

(2)　クライアント PC 上のデータのスマートフォンへの書出し制御設定

シンフォームの社内規程上、業務上の必要性が明確であり、また、他の方法がない場合で、かつ、当該情報の部門責任者の許可及び各部管理責任者の外部メディアの使用許可を得た場合でない限り、クライアントPCを含む社内PC内のデータを外部メディアへ書き出すことを禁止していた。また、運用上も当該行為を制御するシステム（以下「**本件書出し制御システム**」といい、書出し制御機能の設定を「**本件書出し制御設定**」という。）が採用されており、当該システムをバージョンアップさせる際に、本件書出し制御設定の見直しを行っていた。しかし、本件書出し制御システムのバージョンアップの際に、特定の新機種のスマートフォンを含む一部の外部メディアへの書出しについて、書出し制御機能が機能しない状態が生じたため、その事実を知るに至った松崎は、クライアントPC内に保存した

[5] 顧客等の氏名、生年月日、電話番号等の情報を用いて、同一人物の認定を行うことを意味する。

顧客等の個人情報を、松崎所有のスマートフォンに書き出すことができた。このように、松崎による不正行為等に対し、本件書出し制御システムが機能しなかった。

(3) アクセス権限の管理

シンフォームの業務担当者が使用するクライアントPCから本件データベースへアクセスする場合、アクセス権限の付与を受ける必要があった。業務担当者は、管理者の承認を得てアクセス付与申請をし、当該業務担当者が担当する作業に必要であれば、申請受付部門が承認しアクセス権限が付与された。また、シンフォームにおいては、付与済みのアクセス権限の見直しが定期的に行われていない状況も多く見受けられた。

(4) データベース内の情報管理

シンフォームは、本件データベース内の個人情報をより細分化又は階層化しグルーピングした上で、異なるアクセス権限を設定する等の対策までは講じていなかった。また、本件データベースは、主としてマーケティング分析のために使用されていたが、その目的に照らして、必要にして十分な程度までの個人情報の抽象化及び属性化は行われていなかった。

2. 不正行為等の原因となったベネッセグループの体制及びコーポレート・カルチャー

(1) 組織体制の問題点

ベネッセグループにおいては、個人情報にアクセスしうる内部者による情報漏えい等を想定し、本件アラートシステムの設定やログの取得・保存等といった対策を講じてはいたものの、そのような者による情報漏えい等を現実に発生する可能性がある具体的なリスクと想定した上での、二重、三重の対策を講じるといった徹底的な体制までは構築できていなかった。

また、ベネッセグループにおいては、情報セキュリティに関するグループ全体の統括責任者が必ずしも明確に定められていなかったとともに、情報セキュリティについてグループ全体で統括的に管理を行う部署が存在しなかった。

さらに、BC やシンフォームにおいては、ビジネス環境の変化に適応するために頻繁に行われる組織再編の結果、従前行われていた業務が再編後の組織に承継されなかったり、各組織間で責任・権限の所在が不明確になる場合があった。

そのほか、ベネッセグループにおいては、個人情報管理の責任部門が不明確であった。また、内部にて業務に従事する者による不正行為による情報漏えいを防止するためには、高度な専門性を持つ専門家の支援を受けながら厳密な監査を行う必要があったと思われるが、ベネッセグループではそこまでの実効性を持った監査は行われていなかった。シンフォームについてみると、その重要な顧客である BC の事業部門の意向に従わざるを得ない傾向が認められ、BC が、シンフォームの立場を強化するための施策を講じはしたものの、当

該傾向を完全に払拭することはできず、事業効率やスピードを重視せざるを得ない結果、情報セキュリティの維持・向上のために十分な役割を果たせなかった。

(2) 役職員の意識及びコーポレート・カルチャー

ベネッセグループの役職員の多くは、ベネッセグループにおいて、情報セキュリティに多くの予算及びリソースを投入し、また従業員の教育・研修も相当程度行ってきたことから、情報セキュリティについて相当なレベルにあると認識していた可能性が高い。また、ベネッセグループの役職員の多くは、社内の人間が悪意を持って大量の個人情報を持ち出すことはあり得ないという意識を持っていた可能性が高い。このような役職員の意識、ひいてはコーポレート・カルチャーが、ベネッセグループ内部において業務に従事する者の犯行をも想定した徹底した万全の体制を構築できず、不正行為を容認することとなった可能性を否定できない。

Ⅳ. その他の情報処理システムに関する改善点

ベネッセグループ内部において業務に従事する者による不正行為を防止するため、情報処理システムに関するその他の改善を要する点は、以下のとおりである。

1. 業務委託先の管理及びその担当者に対する審査等

シンフォームは、松崎を含め、業務委託先の担当者について、二次委託先、三次委託先等のどの委託先に所属する従業員かというシンフォームとの間の契約上の位置付け等について把握することなく、本件データベースに保存された個人情報等に広範囲にアクセスする権限を付与する場合があった。そのため、シンフォームは、業務委託先の担当者に対する業務の分配や、付与するアクセス権限を必ずしも適切にコントロールできていなかった。特に、個人情報を取扱う等の重要な業務を委託する場合には、個人情報保護の観点から、厳重な管理が行われるべきであった。また、業務担当者による不正行為を想定した十分な行動監視体制を整えるには至っていなかった。

2. 本件データベースへのアクセス・通信ログ等についてのモニタリング方法

シンフォームは、本件データベースについて、業務担当者が使用するクライアントPCからのアクセスについて、自動的にアクセスログを記録し、更に通信ログまで取得していた。これにより、事故が起こった際に、事後的にこれらのログを検証することができたが、意図的な不正行為等を想定してこれらのログを定期的にモニタリングすることは行っていなかった。内部にて業務に従事する者による場合を含め、意図的な不正行為等に対しても万全を期す場合には、上記ログに関する定期的で効果的なモニタリング方法を採用する余地があった。

第3章　再発防止策

Ⅰ．　システムに関する再発防止策

システムに関する問題点に対する再発防止策又は改善策、及び平成26年9月3日時点における対応状況は、以下のとおりである。BHDは、シンフォームのシステムの安全性に関する対策を講じるため、情報セキュリティ会社に対し、システムの安全性に関する改善策の検討を依頼し、シンフォームは同社からの改善提案を受けて対応を行っており、平成26年9月3日時点までに対応が完了した事項も一部存在する。もっとも、大部分は、今後の方針を決定し又は今後の運用を変更したという状況であり、具体的な施策の実施が行われるまで継続的に監視する必要がある。また、シンフォームは、多くの問題点に関し、定期的に監査を実施することを決定しているが、早期に監査を開始し、厳格な運用を行うことが肝要である。

1.　アラートシステムの設定

(1)　再発防止策

シンフォームでは、本件データベースを含む全てのサーバと全てのクライアントPCとの間の通信を本件アラートシステムの対象とする設定変更を完了しているが、当該設定が継続的に適切に行われるためには、その設定対象及び設定手続に関するマニュアル等を作成してシンフォームの担当従業員に周知し、将来における本件アラートシステムの設定漏れを防止する措置を講じる必要がある。具体的には、システムの本番稼働の際のチェックシート等に、本件アラートシステムへの登録という項目を加えることや、BCの委託先監査やシンフォームの内部監査の対象項目として、個人情報を保有するサーバについて当該システムの対象として適切に登録されているか否かを確認する項目を設けること等が考えられる。

(2)　対応状況

本件アラートシステムの設定が、上記のとおり、適切かつ確実に行われるようにするため、シンフォームでは、以下の対応を行っている。

- 本件アラートシステムの設定対象及び設定手続並びに監査対象について、運用マニュアルを作成することとし、その作業中である。
- シンフォームのシステム監査を中立的・専門的に実施する部門としてセキュリティ監査部を新設し、同部を中心として、情報セキュリティ会社の協力を得ながら、本件アラートシステムの設定対象範囲の適切性、運用マニュアルの内容の妥当性及び運用実態等について定期的に監査を実施し、改善指摘を行うことを決定した。また、情報セキュリティ会社の提言を受けて、具体的な実行計画を作成中である。

シンフォームは、組織再編等により担当者や担当部署が変更されても継続的にこれらが

適切に実施されるような体制の構築を構築すべきであり、上記の運用マニュアルを早期に作成することが望まれる。

2. 書出し制御設定

(1) 再発防止策

本件書出し制御設定について、継続的に新しい外部メディアに対応することが必要である。また、外部メディアへの書出しを禁止するという観点からは、クライアントPCの仕様を、外部メディアを一切接続できないものに変更すること[6]やシンクライアント[7]の方式を採用することが考えられる。

(2) 対応状況

社内の情報の外部メディアへの書出しを制御するという観点から、シンフォームでは、以下の対応を行っている。

- 書出し機能を持つ可能性がある全ての外部メディアについて、クライアントPCに物理的に接続した場合及びスマートフォンのテザリング機能等の無線機能を使用した場合のいずれについても、クライアントPCが外部メディアを認識せず、書出しができないように本件書出し制御設定の内容を変更した[8]。
- クライアントPC上にデータを保存させないという観点から、シンクライアントシステムを導入し、クライアントPCへのデータダウンロードができない状態にすることを決定し、既にシンフォームのクライアントPCについては、当該システムの導入が完了した。また、これに併せて、全従業員に対して、各従業員に貸与された社内PCに業務データを保存しないよう改めて注意喚起し、当該PCに業務データが保存されていないことを定期的に確認している。さらに、今後は、社内PCのローカルファイルに保存された業務データの有無を自動検索するソフトを導入する方針である。
- 社内の情報の外部メディアへの書出しについて、スタッフ本部の監査担当者が定期的に監査し、改善指摘を行うことを決定した。

上記の各運用を継続的に実施するため、それぞれの運用をマニュアル等に明記し、組織再編等により、担当者や担当部署が変更されてもこれらが継続的に適切に実施されるような体制を構築するべきである。また、シンクライアントシステムのベネッセグループにお

---

[6] 例えば、USBポートその他の外部メディア接続ポートがないタイプのPCを社内で利用することが考えられる。

[7] システムの利用者が使うPCには最低限の機能しか持たせず、アプリケーションソフトやデータファイル等の資源はサーバで一元管理する方式である。この方式を採用することにより、システム上、クライアントPCのローカルフォルダにデータを保存することが不可能になり、外部メディアへの書出しを防止することができると考えられる。

[8] なお、BCにおいても同様の設定変更が完了している。

ける導入及び社内PCのローカルディスクに保存された業務データの有無を自動検索するソフトの導入については、セキュリティの向上に資するものであり、方針として妥当であるため、早期に導入を実施すべきである。さらに、今後、外部メディアの進歩に対して、適時に十分な対応をとる必要がある。

3. アクセス権限の管理

(1) 再発防止策

業務に必要な範囲を超えて個人情報へのアクセス権限を付与せず、また、不要になったアクセス権限を直ちに削除することが必要である。具体的には、個人情報の内容・属性等に従ってグルーピングし、グループ毎にアクセス権限を設定するといった措置を講じること、業務ごとに必要な一定期間有効となるパスワードでアクセス権限を付与すること、及び定期的にアクセス権限の棚卸しを実施すること等が考えられる。

(2) 対応状況

アクセス権限の管理に関し、シンフォームでは、以下の対応を行っている。

- アクセス権限の棚卸しを実施し、業務上不要なアクセス権限を削除した。
- 付与するアクセス権限を必要最小限にするため、今後は、一定の期間毎にパスワードの更新を行う運用を開始し[9]、また、業務ごとに必要な一定の短い期間にアクセス権限を限定したパスワードを付与する運用とする方針を決定した。
- セキュリティ監査部を新設し、アクセス権限についても、定期的に棚卸しその他の監査を実施し、改善指摘を行うことを決定した。

棚卸しは実施されたものの、継続的にアクセス権限を管理する観点からは、上記の方針が決定され又は一部の運用が実行されているのみであるため、今後の継続的な対応が重要である。必要な期間のみ有効となるパスワードの導入の方針は妥当であり、適切な運用基準を設定の上、早期に導入するべきである。

4. 本件データベース内の情報の管理

(1) 再発防止策

本件データベース内の情報について、個人情報を細分化し、1つのアクセス権限でアクセスできる個人情報の範囲を限定する必要がある。具体的には、個人情報の内容・属性等に従ってグルーピングを行い、グループ毎にアクセス権限を設定するといった措置や、個人情報をその内容により区分し、システム上の管理レベルに差を設け、重要性の高い個人情

[9] 具体的には、一定期間毎にパスワードが更新される運用になり、各アクセス権限は、当該期間の満了時に必要性を判断の上、更新させることとなる。

報にアクセスできる機会を必要最小限にする措置を講じることが考えられる。さらに、本件データベースには、その主たる機能であるマーケティング分析に必要な情報のみを保存し、必要な範囲を超えて個人情報を本件データベースに保存しないことが考えられる。

(2) 対応状況

本件データベース内の情報の適切な管理の実施に関し、シンフォームでは、本件データベースの設計自体を含めて見直しを行っており、本件データベース等マーケット分析のために使用するシステムにおいては個人情報を保有させない方針で具体的な戦略を策定中である。かかる方針は妥当であるため、早期に対応策を具体化し、実施すべきである。

5. その他の情報処理システムに関する改善点

(1) 業務委託先の管理及びその担当者に対する審査等

a. 改善策

シンフォームが、業務の委託先及び再委託先を明確に把握できるように契約上の手当を行い、定期的に監査等を行うべきである。また、少なくとも、個人情報を取扱う等の重要な業務を委託する場合には、当該委託業務を実際に担当する者の履歴書を確認し、必要に応じて面談を実施する等、当該担当者について事前の審査を行うことが望ましい。また、作業に従事する者に対する行動監視について、内部にて業務に従事する者による不正行為を想定した十分な行動監視体制を構築するべきである。

b. 対応状況

業務委託先の管理及びその担当に対する審査等に関し、シンフォームでは、以下の対応を行っている。

- 本番環境を使用する個人情報を取扱うシステム保守･運用業務については、ベネッセグループ外の第三者への業務委託を禁止し、シンフォームの従業員のみにより行う方針である。
- システム開発については、第三者への業務委託を許容するが、業務委託先に対して、二次委託、三次委託等の再委託を原則として禁止し、例外的に、二次委託、三次委託等の再委託を行う場合には、かかる委託の開始前にシンフォームに対して通知を行い、かつ、二次委託、三次委託等の再委託先における勤務実績が 1 年以上存在することその他の再委託先の信用性を確保するための一定の条件を満たす場合に限り許容する旨のガイドラインを作成し、当該ガイドラインを遵守する旨の同意を業務委託先から取得する方針である。
- 業務委託先の担当者には個人情報へのアクセス権限を付与しない方針を決定し、業務委託先の担当者が従来有していた個人情報へのアクセス権限の削除作業は概ね実施済みである。
- 業務委託先に対する監査事項に、二次委託、三次委託等の再委託の有無

を盛り込み、年１回以上の割合で監査を実施することを決定した。

業務委託先の管理等に関する対応等の実施は、現時点では方針等が決定されているのみであり、対応が完了しているものではない。これらはいずれも妥当な対応方針等であり、早期に具体的な施策を決定し、実施すべきである。なお、上記のとおり、業務委託先の担当者に個人情報へのアクセス権限を付与しない方針を決定する等の様々な対応策を導入しているが、業務委託先の担当者等に対する行動監視については、これらの対応策の運用実績を踏まえて実効的な制度を検討し、必要な対策を講じるべきである。

(2)　アクセス・通信ログ等のモニタリング

a.　改善策

本件アラートシステムの閾値をより厳格なものに変更することが考えられる。また、本件アラートシステムの対象として、通信容量を基準とするものだけではなく、通常の業務では使用しない一定の組み合わせのSQLコマンドの入力を基準としたもの等を含めることも考えられる。さらに、このようなシステム上のモニタリングだけではなく、抜打ちで従業員のクライアントPCの操作内容を確認することが考えられる。

b.　対応状況

本件データベースへのアクセス・通信ログ等のモニタリングに関し、シンフォームでは、以下の対応を行っている。

・　本件アラートシステムの閾値の見直しを行った。

・　本件データベースへのアクセス・通信等に対するより効果的なモニタリングが行える仕組みの導入を検討中である。

・　セキュリティ監査部を新設し、ログ監査についても、定期的に監査を実施し、改善指摘を行うことを決定した。

本件アラートシステムについては、上記の閾値変更後の内容で既に運用が開始されているが、業務上必要な通信容量の変化等に応じて、適時に閾値の見直しを行う必要がある。また、より効果的なモニタリング方法を導入する検討を行っている状況であり、早期に対応策を具体化し、実施すべきである。

Ⅱ．　組織体制に関する再発防止策

1.　　内部不正対策の基本方針の策定

ベネッセグループにおいては、内部にて業務に従事する者の不正行為による個人情報の漏えいを想定した徹底した体制を構築していたとはいい難い。今回の不正行為を受け、ベネッセグループとして、そのような者による不正対策に対しても具体的な方針を改めて策定し、これを役職員に周知徹底する必要がある。

2.　　組織上の責任の明確化

ベネッセグループにおいては、情報セキュリティに関するグループ全体の統括責任者及び部署が明らかではなかった。BHD に、情報セキュリティに関するグループ全体の統括責任者及び部署を設置すべきである。そして、統括責任者には、情報セキュリティに関する統括を行うことができる十分な資質・経歴を持った人材を任命する必要がある。

3. 監視機能の組織的強化

ベネッセグループが、失われた信用を回復するためには、再び今回のような大規模な情報漏えい事故が起きることはないと顧客その他の関係者が確信するに足りるだけの措置を講じなければならない。そこで、内部にて業務に従事する者の不正行為による情報漏えいその他の情報漏えいの有無を監視し、これに即座に対応できるよう、情報漏えいに対する厳しい監視を行う組織を設ける必要がある。

そのような部門は、ベネッセグループから再び大規模に情報が漏えいすることをあり得ないものとするとともに、顧客をはじめとする関係者がそのことを信頼できるに値するだけの実効性の高い監視を行うべきである。具体的には、少しの徴候に対してもログを監視し、単なる監視に留まらず、漏えいがないかを積極的に検査する等、このようなチェックをしている限り今回のような大規模な情報漏えいは防止できるという実効性の高い監視を行うべきである。

4. 個人情報に関する組織上の責任の明確化

ベネッセグループにおいては、個人情報をどの部門の責任において管理するのかが明確ではなかった。そこで、業務の全過程において、個人情報の利用・管理に責任を持つ部門（データオーナー）を定め、その権限等を規程上明確にすべきである。そして、個人情報の使用を希望する場合、この部門の承認がなければ、ベネッセグループのいかなる部門においても個人情報を利用できないものとすべきである。

5. 情報セキュリティに関するシンフォームの独立性の確保・向上

シンフォームは、システムの情報セキュリティの維持・向上のために十分な役割を果たせなかった。今後とも、シンフォームが IT システムの開発・運用を行うのであれば、個人情報の保護を含む情報セキュリティの観点から、IT の専門部署として必要な役割を果たすべきである。そのためには、シンフォームに関し、ベネッセグループにおける位置づけ及び組織上・人事上の改革を行う必要がある。

6. 実効的な監査

内部にて業務に従事する者の不正による情報漏えいを防止するためには、高度な専門性を持つ専門家の支援を受けながら厳密な監査を行う必要があったが、ベネッセグループでは、そこまでの実効性を持った監査は行われていなかった。実効性ある監査を行うために

は、その種の情報漏えいを具体的なリスク事象として明確化した上、専門家の助力も得て、これを行う必要がある。

7. 第三者機関の設置

ベネッセグループが信頼を回復するためには、顧客その他の関係者が再び今回のように大規模に情報が漏えいすることがないと確信するに足りる防止策を講じる必要がある。その一つとして、ベネッセグループにおける情報セキュリティの安全性を確認するための第三者機関の設置が考えられる。

当該機関は、①本件のような事案を含む個人情報漏えい事故の再発防止策を含む情報セキュリティ全般について助言・提言すること、②ベネッセグループにおける再発防止策の実施・運用状況を監視すること、及び③これらの助言・提言や再発防止策の監視を通じて、ベネッセグループにおいて個人情報の漏えいがなく、情報セキュリティシステムが安全に機能していることを確認すること等を目的として設置する。当該機関の構成員は、社外の専門家（情報に関する法律・コンプライアンスに関する専門家、情報セキュリティに関する専門家、監査・調査に関する専門家など）等の第三者が考えられる。

Ⅲ. 役職員の意識及びコーポレート・カルチャーに関する再発防止策

ベネッセグループにおいては、情報セキュリティシステムに対する過信や、内部にて業務に従事する者が悪意をもって大量の個人情報を漏えいさせることなどあり得ないといった思いこみが再び生まれないよう、役職員の意識改革に努める必要がある。さらに、ベネッセグループにおいて、再び個人情報漏えい等の企業危機を招来しないよう、今回の出来事を変革の好機と捉え、IT ガバナンスやコーポレート・カルチャーを変革し続ける経営努力が求められる。

以上が本調査委員会の調査報告の概要です。

本調査結果を真摯に受け止め、ベネッセグループでは、以下の再発防止策を策定し、現在既に一部のものについては実行に着手しておりますが、今後さらにこれらの再発防止策を進めて行くことを予定しております。

１．グループ全体の情報管理体制・組織改革について

グループ全体の情報システムのセキュリティレベルの大幅な向上を図るため、IT ガバナンスを強化します。今後、データ・システムについて、データベースの管理、データベースの保守・運用、及びデータベースの利用の 3 つの機能を切り離し、権限・責任を明確化します。そして、3 つの機能の主体が相互に監視・牽制を行う体制とすることで、データ・システムの安全性・健全性を継続的に担保します。

①　データベースの管理：BHD

データベースの管理は、BHD が行います。具体的には、データのセキュリティの管理監督、運用状況の監視・監査、データベースの使用承認等を行います。

組織体制としては、グループ全体の情報管理を含む内部統制・監査に責任を持つ、上席執行役員である CLO（Chief Legal Officer）を設置します。CLO については、グローバル企業にて専門性の高い実績を持つ人材を招へいし、本年 10 月に就任予定です。また、CLO のもと、情報セキュリティについて統括的に管理し、データベースの管理に責任を負う DB 管理本部及びグループ全体の情報セキュリティの監査に責任を持つ CISO（Chief Information Security Officer）を配置します。CISO は、内部不正による情報漏えいを具体的なリスク事象として認識し、新会社（後に定義します。）及び BC に対して実効的な監査を行います。

②　データベースの保守・運用：新たに設立する合弁会社

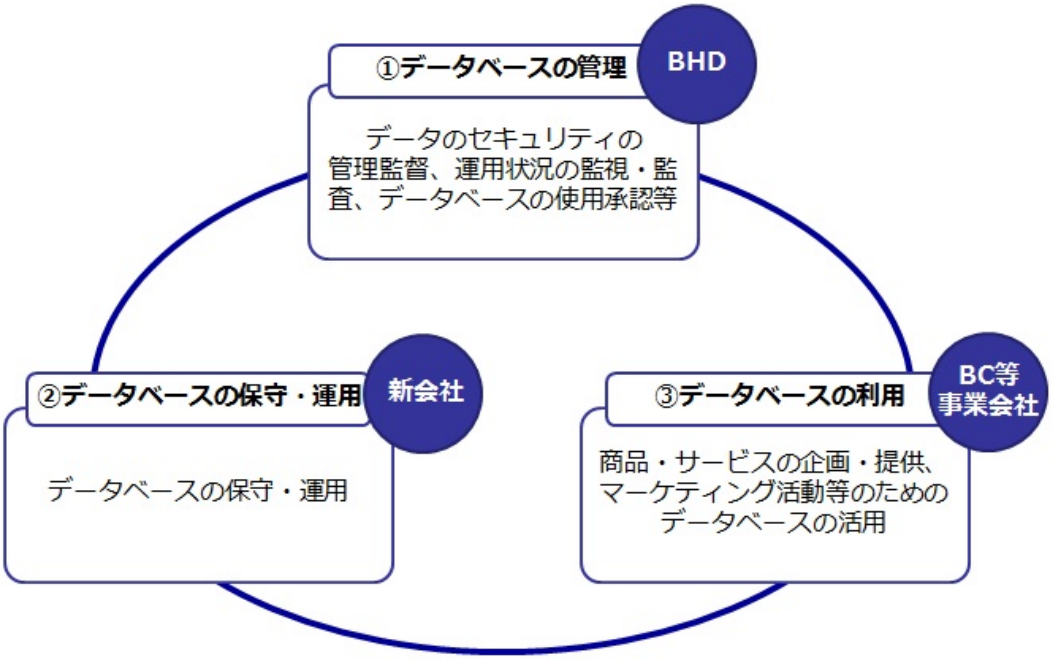
データベースの保守・運用に関しては、新たに BHD と株式会社ラックとの合弁会社（以下、「新会社」といいます。）を設立し、同社にて担当します。新会社により、世界でも有数のセキュリティレベルの高い保守・運用体制を構築することを目指してまいります。この新会社の設立に伴い、これまで保守・運用を担当してきた株式会社シンフォームについては、新合弁会社に、必要とされる資産および人材などの統合を図ります。

新合弁会社は、仮にデータベースを利用するベネッセグループ内の事業会社が事業効率・スピードを優先する意向を有していたとしても、システム運用者として個人情報保護、情報セキュリティの維持・向上に徹してまいります。

③　データベースの利用：BC 等事業会社

ベネッセグループ内の事業会社が、商品・サービスの企画・提供、マーケティング活動等のためのデータベースの活用する際には、BHD・DB 管理本部のガイドライン

を遵守し、必要最小限の範囲で行います。



２．外部監視機関の設置

BHD に外部監視機関を設置し、グループ全体のデータ、システムについて、第三者の視点から定期的かつ客観的な監視・監査（今回の事故の再発防止策を含みます。）を実施する予定です。

当該機関は、①本件個人情報漏えい事実の再発防止策を含む情報セキュリティ全般について助言・提言すること、②ベネッセグループにおける再発防止策の実施・運用状況を監視すること、及び③これらの助言・提言や再発防止策の監視を通じて、ベネッセグループにおいて個人情報の漏えいがなく、情報セキュリティシステムが安全に機能していることを確認すること等を目的として設置します。

外部監視機関は、外部の情報セキュリティや個人情報に関する有識者（情報に関する法律・コンプライアンスに関する専門家、情報セキュリティに関する専門家など）のみで構成し、厳正な監査を行い、お客様の立場に立って公平な判断を下すことを任務とします。その監査結果は、BHD 会長兼社長に助言・提言され、仮に個人情報漏えいのリスクがある場合には迅速に適切な措置を講じてまいります。

３．データベースの保守・運用業務の外部委託について

BC の委託先のうち、特に情報システムの保守・運用については、現在はシンフォームに委託していますが、今後、新会社への委託に移行し、更にセキュリティを向上させる予定です。グループ外への当該業務の委託は行わない方針です。

４．お客様の被害防止に向けた取り組み

お客様への支援を行う専門組織「お客様本部」を、８月４日付で設置いたしました。

お客様の様々な不安解消・低減及び流出した個人情報の拡散防止を目的とした「お客様本部」において、信頼回復に向けて下記の実行施策に継続的に取り組んでまいります。

①　お電話でのお問合わせ対応とお詫び

７月９日の記者会見後、「個人情報に関するお客様お問合わせ窓口（フリーダイヤル）」を開設し、お問合わせへの回答及びお詫びを続けております。

②　お客様情報のオプトアウト・消去対応

保有しているお客様の個人情報に対するオプトアウト・情報消去の申し出をいただいた際は、速やかに対応してまいります。従来のオプトアウト・情報消去に関するBC内ルールの見直しも行います。

③　お客様に向けて他の事業者への対応方法への助言

他の事業者に対するダイレクトメール等の配信停止・情報消去のお申し込みをいただいた際は、その連絡窓口・方法等について、情報提供・アドバイスをいたします（下記、BCホームページご参照）。

http://www.benesse.co.jp/customer/measure1_2.html

④　公的相談機関のご案内

不審な勧誘の例をBCホームページに掲載し、注意を喚起するとともに、不審な勧誘等への対応方法として、最寄りの警察署・消費生活センター等の公的相談機関をご案内しております。

⑤　漏えいした個人情報の利用が疑われる事業者への対応

お客様からの声や独自調査の調査結果等をもとに、漏えいした情報を利用している可能性の高い事業者の把握を行うとともに、利用停止の働きかけを行っております。

⑥　お客様への個別対応

今回の個人情報漏えいによるお客様の様々なお困りごとに対して、個別に相談に応じています。お客様個別のご事情に合わせ、具体的な解決に向けたノウハウの提供や、カウンセラーの導入も行っております。

⑦　外部機関と連携した恒久的取り組み

お客様や各省庁、その他の専門機関、事業会社等と連携した個人情報漏えいの恒久的な発生防止・拡散防止のための活動への支援や主体的参画を、検討・実施する予定です。

以　上