

埼玉県社会保険労務士会大宮支部

研修会資料

個人情報保護法関係研修会

内容

資料 1	プライバシーポリシーの例.....	1
資料 2	(小規模事業用) 個人情報保護規程例	5
資料 3	漏えい等事例	18

弁護士 坂 東 利 国

 東京エクセル法律事務所
LAW FIRM

資料1 プライバシーポリシーの例

(網掛け部分は令和2年改正を受けた加筆・修正箇所)

個人情報等の保護に関する基本方針

株式会社 ●●●●（以下「当社」といいます。）は、個人情報の取扱いが安全かつ適正に行われるよう取り組むことが企業の社会的責務であると考え、以下の基本方針に従って、個人情報を適切に取り扱います。

1. 関係法令・ガイドライン等の遵守

当社は、個人情報に関して適用される法令、ガイドラインその他の規範（以下、「個人情報関係法令等」といいます。）を遵守します。

2. 定義

- (1) この基本方針において、「個人情報」、「個人データ」、「保有個人データ」、「仮名加工情報」、「匿名加工情報」および「個人関連情報」の意味については、個人情報の保護に関する法律（以下「個人情報保護法」といいます。）の定めるところによるものとします。
- (2) この基本方針において、「パーソナルデータ」とは、生存する個人に関する情報をいい、「個人情報」、「個人データ」、「保有個人データ」、「仮名加工情報」、「匿名加工情報」および「個人関連情報」から構成されます。

3. 適用

- (1) この基本方針は、当社が、業務上取得するパーソナルデータの取り扱いに適用します。
- (2) 特定のパーソナルデータの種類によって、当社が、このポリシーとは別にルールを定めている場合、このポリシーのほか当該ルールを適用します。なお、当該ルールがこのポリシーと矛盾抵触する場合は、その限度で、当該ルールをこのポリシーに優先して適用します。

4. パーソナルデータの取得と利用

当社は、パーソナルデータを適法かつ公正な手段により取得するとともに、違法または不当な行為を助長し、または誘発するおそれがある方法によりパーソナルデータを利用しません。

5. 個人情報の利用目的

- (1) 当社が取り扱う個人情報の利用目的には、以下のものが含まれます。その他、個別の利用目的がある場合には、別途公表します。

[利用目的の例1]

- ① お客様の情報
 - ・ 当社が取り扱う商品および新商品に関する情報ならびにサービスの提供
 - ・ 当社が取り扱う商品の発送および問い合わせの対応
 - ・ 当社が提供するサービスの改善および新規開発、ならびにアンケート等の意向調査の実施および分析
 - ・ キャンペーン、展示会、イベントその他の当社商品および新商品、ならびに当社が提供するサービスおよび新サービスに関するご案内発送および運営
 - ・ 当社商品のインターネットショップ、通信販売等の運営

- ・ 当社の事業・サービスに関する問い合わせへの対応
 - ・ その他、これらの業務に密接に関連する業務
- ② 採用応募者の情報
- ・ 採用応募者の受け付け、採否の検討および連絡
 - ・ その他、これらの業務に密接に関連する業務
- ③ お取引先の情報
- ・ 当社取扱商品及び新商品に関する情報ならびにサービスの提供
 - ・ 商品、技術およびサービスの共同開発の実施ならびに連絡
 - ・ 商談の実施および連絡
 - ・ 委託された業務の遂行
 - ・ 当社が管理する施設の入退館の管理およびセキュリティの確保
 - ・ その他、これらの業務に密接に関連する業務
- ④ 元従業員・退職者の個人情
- ・ 退職者的人事労務業務（福利厚生を含みます）および懇親等の必要に応じた連絡
 - ・ その他、これらの業務に密接に関連する業務

[利用目的の例 2]

① 事業に関する目的

- ・ 当社が取り扱う商品の発送、関連するアフターサービスおよび新商品・サービスに関する情報のお知らせ
- ・ 当社が提供するサービスの改善および新規開発、ならびにアンケート等の意向調査の実施

② 調査・分析の目的

- ・ 当社の事業・サービスの利用者その他の取引先における当社事業・サービスの利用状況の把握・分析、およびアンケート等の意向調査の実施のため

③ インターネットサービスに関する目的

- ・ ログインが必要なサービスにおける利用申請の受け付け、本人確認および利用者認証、インターネットサービスの改善および新規開発、ならびにインターネットサービスの安定的な提供

④ その他の目的

- ・ ご挨拶
- ・ 物品または役務の調達
- ・ 採用応募者の受け付け、採否の検討および連絡
- ・ 当社が管理する施設の入退館の管理およびセキュリティの確保
- ・ 当社の事業・サービスに関する問い合わせへの対応

(2) 当社は、その取り扱う個人情報の利用目的（変更された利用目的を含みます）を、適切な場所とタイミングで、本人に通知し、または公表します。

(3) 当社は、個人情報保護法で認められている場合を除き、あらかじめ本人の同意を得ないで、個人情報を、その利用目的の達成に必要な範囲を超えて取り扱いません。

6. 第三者提供等

(1) 当社は、個人情報保護法で認められている場合を除き、あらかじめ本人の同意を得ないで、個人データ

タを第三者に提供しません。

- (2) 当社は、個人データの取り扱いを委託する場合、適正に取り扱うことができる委託先を選び、委託先でも適切な安全管理が講じられるよう、必要な監督を行います。

7. 開示等請求への対応

当社は、本人から保有個人データの開示、訂正、追加または削除、利用停止等の請求を受けた場合には、個人情報関係法令等および当社の規程に従い合理的な期間と妥当な範囲内でこれに対応します。

8. 仮名加工情報の取扱い

- (1) 当社は、仮名加工情報を作成するときは、個人情報関係法令等の定めに従い、適切な措置を講じます。
- (2) 当社は、法令に基づく場合を除くほか、仮名加工情報を第三者に提供しません。
- (3) 当社は、仮名加工情報を取り扱うにあたって、当該仮名加工情報の作成の元となった個人情報の本人を識別する目的で、当該仮名加工情報を他の情報と照合することは行いません。
- (4) 当社は、仮名加工情報を取り扱うにあたって、電話、信書便の送付、メール送信または訪問等のために、仮名加工情報に含まれる連絡先その他の情報を利用しません。

9. 仮名加工情報の利用目的

- (1) 当社が取り扱う仮名加工情報の利用目的には、以下のものが含まれます。

[利用目的の例]

- ① 事業・サービスの開発・改善
 - ・ 当社の事業・サービスの運用・保守に関する状況の分析
 - ・ 当社の事業・サービスにおける不正防止のための分析
- ② 事業・サービスの安定性の確保
 - ・ 当社の事業・サービスの利用者その他の取引先における当社事業・サービスの利用状況に関する傾向の分析
 - ・ 当社および当社の事業・サービスの利用者その他の取引先からのご相談やお問い合わせの分析
- ③ その他の目的
 - ・ 社会課題の解決や、お客様の満足度向上のためのビッグデータ利活用に関する分析
 - ・ 当社および当社のグループ企業各社の業務改善のための分析

- (2) 当社は、その取り扱う個人情報である仮名加工情報の利用目的(変更された利用目的を含みます)を、適切な場所とタイミングで公表します。
- (3) 当社は、個人情報である仮名加工情報を、法令に基づく場合を除くほか、その利用目的の達成に必要な範囲を超えて取り扱いません。

10. 匿名加工情報の取扱い

- (1) 当社は、匿名加工情報を作成するときは、個人情報関係法令等の定めに従い、適切な措置を講じます。
- (2) 当社は、匿名加工情報を作成したときは、当該匿名加工情報に含まれる個人に関する情報の項目を、適切な場所とタイミングで公表します。
- (3) 当社は、その作成した匿名加工情報を取り扱うにあたって、当該匿名加工情報の作成の元となった個人情報の本人を識別する目的で、当該匿名加工情報を他の情報と照合することは行いません。
- (4) 当社は、他の者が作成した匿名加工情報を取り扱うにあたって、当該仮名加工情報の作成の元となっ

た個人情報の本人を識別する目的で、作成の元となった個人情報から削除された情報または加工の方法に関する情報を取得し、または当該匿名加工情報を他の情報と照合することは行いません。

- (5) 当社は、匿名加工情報を第三者に提供するときは、あらかじめ、第三者に提供される匿名加工情報に含まれる個人に関する情報の項目およびその提供の方法について、適切な場所とタイミングで公表するとともに、当該第三者に対して、当該提供に係る情報が匿名加工情報である旨を明示します。

11. 安全管理措置に関する事項

当社は、その取り扱うパーソナルデータの性質および量、パーソナルデータを記録した媒体の性質等に起因するパーソナルデータの漏えい、滅失または毀損のリスクに応じて、パーソナルデータの漏えい、滅失または毀損の防止その他のパーソナルデータの適切な安全管理のために必要かつ適切な措置を講じます。

12. 質問及び苦情処理の窓口

当社は、対応する窓口にいただいたパーソナルデータに関する問い合わせや苦情等に対して、個人情報お問い合わせ窓口において、適切かつ誠実、迅速に対応いたします。

13. 外国法の適用

当社が保有するパーソナルデータのうち、その取り扱いについて外国法の適用を受ける情報の取り扱いについては、当該外国法を順守して取り扱います。

14. 個人情報お問い合わせ窓口

〒 000-0000

●●県●●市●●町0丁目0－0

電話：00-0000-0000

株式会社 ●●●● 個人情報お問い合わせ窓口

※ お電話での受付は、当社営業日の午前10時から午後5時（お昼休みを除く）とさせていただきます。

※ ご来社による請求はお受けいたしかねますのでご了承下さい。

制定日 ●●●●年●●月●●日

最終改定日 ●●●●年●●月●●日

株式会社 ●●●●

代表取締役 ●● ●●

資料2（小規模事業用）個人情報保護規程例

（網掛け部分は令和2年改正を受けた加筆・修正箇所。なお、仮名加工情報、匿名加工情報および個人関連情報は取り扱わないことを前提としているため、これらに関する条項はない。）

個人情報保護規程

制定 年 月 日

株式会社○○○○○

第1章 総則

（目的）

第1条 本規程は、当社において、従業者による個人情報の取扱いが安全かつ適正に行われるよう従業者が遵守すべき事項を定めることを目的とする。

（定義）

第2条 本規程において、各用語の定義は次の通りとする。

1 法

個人情報の保護に関する法律（平成十五年五月三十日法律第五十七号）

2 政令

個人情報の保護に関する法律施行令（平成十五年十二月十日政令第五百七号）

3 個人情報保護委員会規則

個人情報の保護に関する法律施行規則（平成28年10月5日個人情報保護委員会規則第3号）

4 個人情報

生存する個人に関する情報であって、次の各号のいずれかに該当するもの。

(1) 当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）。

(2) 個人識別符号が含まれるもの。

5 個人識別符号

当該情報単体から特定の個人を識別できる文字、番号、記号その他の符号であって、政令で定めるもの。

6 個人情報データベース等

個人情報を含む情報の集合物であって、次の各号のいずれかに該当するもの。

(1) 特定の個人情報をコンピュータ（電子計算機）を用いて検索することができるよう体系的に構成したもの。

(2) 前号に掲げるもののほか、特定の個人情報を容易に検索することができるよう体系的に構成したものとして政令で定めるもの。

上記各号に該当する個人情報を含む情報の集合物であっても、次の各号のいずれにも該当す

るものは、個人情報データベース等から除外する。

- (1) 不特定かつ多数の者に販売することを目的として発行され、かつ、その発行が法に違反して行われたものでないこと。
- (2) 不特定かつ多数の者により隨時に購入することができ、又はできたものであること。
- (3) 生存する個人に関する他の情報を加えることなくその本来の用途に供しているものであること。

7 個人データ

個人情報データベース等を構成する個人情報

8 保有個人データ

当社が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことができる権限を有する個人データ。ただし、次の各号のいずれかに該当するものは除く。

- (1) 当該個人データの存否が明らかになることにより、本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの。
- (2) 当該個人データの存否が明らかになることにより、違法又は不法な行為を助長し、又は誘発するおそれのあるもの。
- (3) 当該個人データの存否が明らかになることにより、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれのあるもの。
- (4) 当該個人データの存否が明らかになることにより、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの。

9 要配慮個人情報

本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう。

10 本人

個人情報によって識別される特定の個人

11 従業者

当社の組織内にあって、直接又は間接に当社の指揮監督を受けて、当社の業務に従事している者をいい、当社と雇用関係にある従業員のみならず、取締役、執行役、理事、監査役、監事、派遣社員も含まれる。

12 漏えい等

当社が取り扱う個人情報について、外部に流出すること（漏えい）、内容が失われること（滅失）、又は内容が意図しない形で変更され、若しくは内容を保ちつつも利用不能な状態となること（毀損）。

13 漏えい等事案

当社が取り扱う個人情報の漏えい、滅失、毀損その他の個人情報の安全の確保に係る事態（漏えい等又はそのおそれのある事案）

第2章 安全管理措置

第1節 総則

(安全管理措置)

第3条 当社は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの適切な管理のために必要な安全管理措置を講ずる。

第2節 組織的の安全管理措置及び人的の安全管理措置

(個人情報取扱担当者)

第4条 当社が扱うことのできる個人データの取得・利用、保管・管理及び第三者提供その他の個人データの取扱いを行う従業者を個人情報取扱担当者とし、個人情報取扱担当者は明確にしなければならない。

- 2 個人情報取扱担当者は、個人情報の取扱いに関する留意事項について、定期的に教育研修を受けなければならない。
- 3 個人情報取扱担当者は、個人情報に関する法令及び当社諸規程並びに個人情報取扱責任者その他上長の指示に従って、個人情報を取り扱わなければならない。
- 4 個人情報取扱担当者は、当社における個人データの取扱いに関し、漏えい等事案又は法令若しくは当社諸規程に違反する行為の発生若しくはそのおそれを把握した場合は、直ちに個人情報取扱責任者又は部門長に報告しなければならない。

(個人情報取扱責任者)

第5条 当社は、個人情報の取扱いの管理に関する事項を行うために必要な知識及び経験を有していると認められる従業者のうちから個人情報取扱責任者を任命する。

- 2 個人情報取扱責任者は、次に掲げる権限と責任を有する。
 - (1) 個人情報取扱担当者に対する必要かつ適切な監督
 - (2) 個人データの取扱状況の記録及びその管理
 - (3) 個人データの取扱いを外部に委託する場合の委託先の選定、委託契約締結の承認、委託先における個人データの取扱状況の把握
 - (4) 本規程その他当社諸規程に規定された取扱方法に従って個人データが取り扱われていることの確認
 - (5) 個人データの取扱状況の定期的な点検
- 4 個人情報取扱責任者は、当社における個人データの取扱いに関し、漏えい等事案又は法令若しくは当社諸規程に違反する行為の発生若しくはそのおそれを把握した場合は、直ちに当社役員に報告しなければならない。

(部門長の責務)

第6条 部門長は、当該部門が取り扱う個人情報を適切に管理する任に当たる。

- 2 部門長は、当社における個人データの取扱いに関し、漏えい等事案又は法令若しくは当社諸規程に違反する行為の発生若しくはそのおそれを把握した場合は、直ちに個人情報取扱責任者又は当社役員に報告しなければならない。

(従業者の責務)

第7条 従業者は、当社が取り扱う個人情報について、当社の業務に従事している間だけでなく、退職後も、他の従業者その他第三者に開示漏えいしてはならず、自己のため又は第三者のために

使用してはならない。

- 2 当社は、従業者に対して、個人情報の保護及び適正な取扱いに関する誓約書の提出を求めることができる。
- 3 従業者は、当社が決定した方針に基づく研修を受けなければならぬ。
- 4 従業者は、当社における個人データの取扱いに関し、漏えい等事案又は法令若しくは当社諸規程に違反する行為の発生若しくはそのおそれを把握した場合は、直ちに部門長又は個人情報取扱責任者に報告しなければならない。

(点検・監査)

第8条 当社は、個人データの取扱状況の点検及び監査を、次の各号に掲げる事項を参考し、適宜の方法で実施するものとする。

- (1) 個人データを取り扱う部署において、自ら個人データの取扱状況を点検する。
 - (2) 個人データの取扱状況を他部署が定期的に点検し、個人データの取扱いが適法かつ適切に行われているかについて監査する。
 - (3) 個人データの取扱状況を個人情報取扱責任者が定期的に点検し、個人データの取扱いが適法かつ適切に行われているかについて監査する。
 - (4) 当社から独立しあつ情報セキュリティについて専門的な知見を有する第三者による個人データの取扱状況の監査を受ける。
- 2 前項による点検及び監査の結果は、当社代表者に報告する。

(見直し)

第9条 当社代表者は、前条の点検及び監査の結果のほか、個人情報の取扱いに関する法令の制定・改正及び社会情勢の変化等に応じて、定期的に安全管理措置の見直し及び改善を行う。

(漏えい等事案への対応)

第10条 当社は、当社が取り扱う個人データの漏えい等事案が発生した場合は、次の各号に掲げる措置を講じる。

- (1) 個人情報取扱責任者及び当社代表者への速やかな報告及び漏えい等事案による被害の拡大を防止するために必要な措置
- (2) 漏えい等事案の事実関係の調査及び原因の究明に必要な措置
- (3) 事実調査で把握した事実関係による事故の影響範囲の特定のために必要な措置
- (4) 事実調査の結果を踏まえ、漏えい等事案の再発防止策の検討及び実施に必要な措置
- (5) 法第26条第1項に従った個人情報保護委員会への報告及び法第26条第2項に従った本人への通知の実施

(監督及び教育研修)

第11条 当社は、個人情報が当社諸規程に基づき適正に取り扱われるよう、個人情報取扱担当者に対する必要かつ適切な監督を行う。

- 2 当社は、個人情報の取扱いに関する当社諸規程を従業者に遵守させ、個人情報の適正な取扱いに関する従業者の意識を高めるための啓発その他の教育研修を実施する。

第3節 物理的の安全管理措置

(物理的の安全管理措置)

第12条 当社は、個人データを取り扱う区域の適切な管理並びに個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するための適切な管理により、個人データを取り扱うことのできる従業者以外の者が容易に個人データを閲覧等できないようにする措置を講ずる。

- 2 当社は、個人データが記録された電子媒体又は個人データが記載された書類等を持ち運ぶ場合に、個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するための方策を講ずる。
- 3 当社が個人データを削除し、又は個人データが記録された機器若しくは電子媒体等を廃棄したときは、確実に削除又は廃棄したことを個人情報取扱責任者が確認する。

第4節 技術的の安全管理措置

(技術的の安全管理措置)

第13条 当社は、個人情報取扱担当者その他の個人データを取り扱うことのできる機器及び当該機器を取り扱う従業者を明確化し、個人データへの不要なアクセスを防止する措置を講じる。

- 2 当社は、個人情報取扱担当者その他の個人データを取り扱う情報システムを使用する従業者が正当なアクセス権を有する者であることを、識別・認証する。
- 3 当社は、個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用する。
- 4 当社は、情報システムの使用に伴う個人データの漏えい等を防止するための措置を講じ、適切に運用する。

第5節 委託先の監督

(委託先の監督)

第14条 当社が個人データの取扱いを外部に委託する場合は、当該委託において取り扱う個人データの安全管理が図られるよう、当該委託を受けた者（以下、「委託先」という。）に対する必要かつ適切な監督を行わなければならない。

第3章 個人情報等の取扱い

第1節 取得・利用

(利用目的の特定)

第15条 当社が個人情報を取り扱うにあたっては、その利用目的をできる限り特定しなければならない。

- 2 当社が個人データを第三者に提供する場合は、前項により特定する利用目的においてその旨を特定しなければならない。
- 3 当社が第1項により特定した利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行ってはならない。

(個人情報の利用目的による制限)

第16条 当社は、あらかじめ本人の同意を得ないで、前条の規定により特定した利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

- 2 当社は、合併その他の事由により他の者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。
- 3 前2項の規定は、次の各号のいずれかに該当する場合は、適用しない。
 - (1) 法令に基づく場合
 - (2) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
 - (3) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
 - (4) 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
 - (5) 学術研究機関に学術研究などの目的で個人情報を取り扱う必要があり、個人の権利利益を不当に侵害するおそれがない場合として、法第18条1項5号及び6号が定める場合

(不適正な利用の禁止)

第17条 当社は、違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない。

(適正な取得)

第18条 当社は、個人情報を、偽りその他不正の手段により取得してはならない。

(要配慮個人情報の取得制限)

第19条 当社は、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。

- 2 前項の規定は、次の各号のいずれかに該当する場合は、適用しない。
 - (1) 法令等に基づく場合
 - (2) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
 - (3) 公衆衛生の向上又は児童の健全な育成の推進のため特に必要がある場合であって、本人の同意を得ることが困難であるとき。
 - (4) 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
 - (5) 本人、国の機関、地方公共団体又は報道機関等により公開されている場合
 - (6) 目視又は撮影により、外形上明らかな要配慮個人情報を取得する場合
 - (7) 委託又は事業承継等により、要配慮個人情報の提供を受けるとき。
 - (8) その他、法及び政令が定める場合

(個人情報の取得に際しての利用目的の通知等)

- 第20条 当社が個人情報を取得する場合は、あらかじめ、個人情報の利用目的を公表し、あらかじめ公表できない場合は、取得後速やかに、その利用目的を本人に通知し、又は公表しなければならない。
- 2 当社が、契約書・申込書・アンケートその他の書面(電子メール等の電磁的記録も含む。)により本人から直接個人情報を取得する場合は、あらかじめ、本人に対して、書面(電磁的記録

も含む。)により、その利用目的を明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

3 前2項の規定は、次の各号のいずれかに該当する場合は、適用しない。

- (1) 人の生命、身体又は財産その他の権利利益を保護するため必要な場合
- (2) 当社の権利又は正当な利益を害するおそれがある場合
- (3) 国又は地方公共団体の法令に定める事務の遂行に支障を及ぼすおそれがある場合
- (4) 取得の状況に照らし、利用目的が明らかであると認められる場合

第2節 保管・管理

(個人データの正確性の確保)

第21条 当社は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努める。

(個人データの消去)

第22条 当社は、個人データを利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努める。

2 前項の規定にかかわらず、個人情報が記載された書類等について、所管法令により一定期間の保存が義務付けられている場合は、その期間は当該個人情報を保管しなければならない。

(漏えい等の報告)

第23条 当社は、当社が取り扱う個人データの漏えい等事案であって、次の各号のいずれかに該当する事態(以下、「報告対象事態」という。)を知ったときは、個人情報保護委員会に対し、報告対象事態を知った時点から5日以内に、次項各号で定める事項(以下、「報告事項」という。)のうち当該時点において把握している事項を速報として報告するとともに、個人情報保護委員会規則で定める報告期限内に、報告事項の全てを確報として報告しなければならない。

- (1) 要配慮個人情報が含まれる個人データの漏えい等が発生し、又は発生したおそれがある事態
- (2) 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
- (3) 不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
- (4) 個人データに係る本人の数が1000人を超える漏えい等が発生し、又は発生したおそれがある事態

2 当社が報告対象事態を知ったときは、次の各号に定める事項を個人情報保護委員会に報告する。

- (1) 当該事態の発生日、発覚日、発生事案、発見者、報告対象事態該当性、委託元・委託先の有無及び事実経過その他の当該事態の概要
- (2) 漏えい等が発生し、又は発生したおそれがある個人データの項目並びに媒体及び種類(顧客情報又は従業員情報の別その他の事項)
- (3) 漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数
- (4) 当該事態が発生した原因及び当該事態が発生した主体(報告者又は委託先)
- (5) 当該事態に起因して発生する二次被害又はそのおそれの有無及びその内容
- (6) 当該事態を知った後、本人に対して行った措置(通知を含む。)の実施状況

(7) 当該事態に関する公表の実施状況

(8) 漏えい等事案の再発防止のために講ずる措置（実施済みの措置と今後実施予定の措置）

(9) 前各号の事項を補完する上で参考となる事項

3 前2項の規定は、漏えい等が発生し、又は発生したおそれがある個人データについて、高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じている場合は、適用しない。

(漏えい等の本人への通知)

第24条 当社は、報告対象事態を知ったときは、当該事態の状況に応じて速やかに、当該本人の権利利益を保護するために必要な範囲において、前条第2項第(1)号、(2)号、(4)号、(5)号および(9)号に定める事項を本人に通知しなければならない。

2 前項の規定は、本人への通知が困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、適用しない。

第3節 第三者提供

(個人データの第三者提供の制限)

第25条 当社は、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

2 前項の規定は、次の各号のいずれかに該当する場合は、適用しない。

(1) 法令に基づく場合

(2) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

(3) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

(4) 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

(5) 学術研究機関に学術研究などの目的で個人情報を取り扱う必要があり、個人の権利利益を不当に侵害するおそれがない場合として、法第27条第1項第5号から7号が定める個人データの提供に該当する場合

3 次の各号のいずれかに該当する場合は、個人データの提供を受ける者は、前各項の適用については、第三者に該当せず、当社は、あらかじめ本人の同意を得ないで、その者に個人データを提供できる。

(1) 個人データの取扱いの全部又は一部の委託に伴って当該個人データを提供するとき。

(2) 合併その他の事由による事業の承継に伴って個人データを提供するとき。

(3) 法第27条第5項第3号が定める共同利用により個人データを提供するとき。

(外国にある第三者への個人データの提供の制限)

第26条 当社は、本邦の域外にある国又は地域（以下、「外国」という。）にある第三者に個人データを提供する場合には、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。

2 前項の規定は、前条第2項各号のいずれかに該当する場合は、適用しない。

3 第1項の規定は、個人の権利利益を保護する上で我が国と同等の水準にあると認められる個

人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定める外国にある第三者に個人データを提供する場合は適用しない。この場合においては、個人データの提供は前条の規定に従う。

- 4 第1項の規定は、外国にある事業者のうち、個人データの取扱いについて法により本邦にある事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している者に個人データを提供する場合には適用しない。この場合においては、個人データの提供は前条の規定に従う。

(第三者提供に係る記録の作成等)

第27条 当社は、個人データを第三者に提供したときは、当該個人データを提供した年月日、当該第三者の氏名又は名称その他の個人情報保護委員会規則で定める事項に関する記録を作成し、当該記録を作成した日から個人情報保護委員会規則で定める期間保存しなければならない。

- 2 前項の規定は、第25条第1項の規定による第三者への個人データの提供にあっては、同条第2項各号又は第3項各号のいずれかに該当する場合は適用せず、当社は記録を作成することを要しない。
- 3 第1項の規定は、前条第1項の規定による外国にある第三者への個人データの提供にあっては、同条第2項各号のいずれかに該当する場合は適用せず、当社は記録を作成することを要しない。
- 4 次の各号のいずれかに該当する者は、第1項の適用については、第三者に該当せず、当社は、これらの者に個人データを提供した場合の記録を作成することを要しない。
- (1) 国の機関
 - (2) 地方公共団体
 - (3) 独立行政法人等
 - (4) 地方独立行政法人

(第三者提供を受ける際の確認等)

第28条 当社は、第三者から個人データの提供を受けるに際しては、次の各号に掲げる事項の確認を行わなければならない。

- (1) 当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名
 - (2) 当該第三者による当該個人データの取得の経緯
- 2 前項の規定は、当該個人データの提供が第27条第2項各号又は第3項各号のいずれかに該当する場合は適用せず、当社は確認を行うことを要しない。
- 3 次の各号のいずれかに該当する者は、第1項の適用については、第三者に該当せず、当社は、これらの者から個人データの提供を受ける場合の確認を行うことを要しない。
- (1) 国の機関
 - (2) 地方公共団体
 - (3) 独立行政法人等
 - (4) 地方独立行政法人
- 4 当社は、第1項の規定による確認を行ったときは、個人情報保護委員会規則で定める事項に関する記録を作成し、当該記録を作成した日から個人情報保護委員会規則で定める期間保存しなければならない。

第4章 開示等の請求等

(保有個人データに関する事項の本人への周知)

第29条 当社は、保有個人データに関し、次の各号に掲げる事項を、本人の知り得る状態に置くものとする。本人の知りうる状態は、本人の求めに応じて遅滞なく回答する場合を含む。

- (1) 当社の名称、住所及び代表者の氏名
- (2) 全ての保有個人データの利用目的（第20条第3項第(1)号から第(3)号のいずれかに該当する場合を除く。）
- (3) 第30条から36条の規定による請求に応じる手続並びに第30条による利用目的の通知の求め及び第31条による開示請求を受けたときの手数料の額を定めたときは手数料の額
- (4) 法第23条の定めにより保有個人データの安全管理のために講じた措置
- (5) 当社が認定個人情報保護団体の対象事業者である場合は、当該認定個人情報保護団体の名称及び苦情の申出先

(保有個人データの利用目的の通知の求め)

第30条 当社は、本人から、当該本人が識別される保有個人データの利用目的の通知を求められたときは、直ちに、当該請求に係る保有個人データの利用目的の通知の可否を判断しなければならない。

- 2 当社は、前項の規定による求めに対し、次の各号のいずれかに該当する場合は、利用目的を通知しないことができる
 - (1) 前条の規定による全ての保有個人データの利用目的の周知により、当該本人が識別される保有個人データの利用目的が明らかな場合
 - (2) 第20条第3項第(1)号から第(3)号のいずれかに該当する場合
- 3 当社は、第1項の規定による求めに係る保有個人データの利用目的を通知する旨の決定をしたときは、本人に対し、遅滞なく、当該保有個人データの利用目的を通知しなければならない。
- 4 当社は、第1項の規定による求めに係る保有個人データの利用目的を通知しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

(保有個人データの開示請求)

第31条 当社は、本人から、当該本人が識別される保有個人データの開示請求を受けたときは、直ちに、当該請求に係る保有個人データの開示の可否及び本人が請求した方法による開示の可否を判断しなければならない。

- 2 当社は、前項の請求により保有個人データを開示することにより次の各号のいずれかに該当する場合は、その全部又は一部を開示しないことができる。
 - (1) 本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
 - (2) 当社の業務の適正な実施に著しい支障を及ぼすおそれがある場合
 - (3) 他の法令に違反することとなる場合
- 3 当社は、第1項の規定による請求に係る保有個人データを開示する旨の決定をしたときは、本人に対し、遅滞なく、当該保有個人データを開示しなければならない。
- 4 当社は、第1項の規定による請求に係る保有個人データの全部若しくは一部について開示しない旨の決定をしたとき、当該保有個人データが存在しないとき、又は同項の規定により本人が請求した方法による開示が困難であるときは、本人に対し、遅滞なく、その旨を通知しなければならない。

(第三者提供記録の開示請求)

第32条 当社は、本人から、当該本人が識別される個人データに係る第27条及び第28条で定める記録（以下、「第三者提供記録」という。）の開示請求を受けたときは、直ちに、当該請求に係る第三者提供記録の開示の可否及び本人が請求した方法による開示の可否を判断しなければならない。

2 次の各号に該当するものは、第三者提供記録から除外する。

- (1) 当該記録の存否が明らかになることにより、本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの。
- (2) 当該記録の存否が明らかになることにより、違法又は不当な行為を助長し、又は誘発するおそれがあるもの。
- (3) 当該記録の存否が明らかになることにより、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあるもの。
- (4) 当該記録の存否が明らかになることにより、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの。

3 当社は、前項の規定による請求に係る第三者提供記録を開示する旨の決定をしたときは、本人に対し、遅滞なく、当該第三者提供記録を開示しなければならない。

4 当社は、第1項の規定による請求に係る第三者提供記録の全部若しくは一部について開示しない旨の決定をしたとき、当該第三者提供記録が存在しないとき、又は同項の規定により本人が請求した方法による開示が困難であるときは、本人に対し、遅滞なく、その旨を通知しなければならない。

(保有個人データの訂正等の請求)

第33条 当社は、本人から、当該本人が識別される保有個人データの内容が事実でないとして、当該保有個人データの訂正、追加又は削除（以下、「訂正等」という。）を請求された場合には、直ちに、必要な調査を行わなければならない。

2 当社は、前項の規定による調査の結果、当該保有個人データの内容が事実でないと判断される場合は、当該保有個人データの訂正等をしなければならない。

3 当社は、第1項の規定による請求に係る保有個人データの内容の全部若しくは一部について訂正等を行ったとき、又は訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨（訂正等を行ったときは、その内容を含む。）を通知しなければならない。

(保有個人データの利用停止等の請求)

第34条 当社は、本人から、当該本人が識別される保有個人データについて、法第18条の規定に違反する個人情報の目的外利用、法第19条の規定に違反する個人情報の不適正な利用、法第20条第1項の規定に違反する個人情報の不正の手段による取得、又は法第20条第2項の規定に違反する要配慮個人情報の取得が行われているとして、当該保有個人データの利用の停止又は消去（以下、「利用停止等」という。）の請求を受けた場合には、直ちに、当該請求に理由があるかの調査を行わなければならない。

2 当社は、前項の規定による保有個人データの利用停止等の請求に理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければならない。ただし、当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要な

これに代わるべき措置をとるときは、この限りでない。

- 3 当社は、第1項の請求に係る保有個人データの全部又は一部について利用停止等を行ったとき若しくは利用停止等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

(保有個人データの第三者提供停止の請求)

第35条 当社は、本人から、当該本人が識別される保有個人データについて、法第27条又は法第28条の規定に違反して第三者に提供されているとして、当該保有個人データの第三者提供停止の請求を受けた場合には、直ちに、当該請求に理由があるかの調査を行わなければならない。

- 2 当社は、前項の規定による保有個人データの第三者提供停止の請求に理由があることが判明したときは、遅滞なく、当該保有個人データの第三者への提供を停止しなければならない。ただし、当該保有個人データの第三者への提供の停止に多額の費用を要する場合その他の第三者への提供を停止することが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。
- 3 当社は、第1項の請求に係る保有個人データの全部又は一部について第三者への提供を停止したとき若しくは第三者への提供を停止しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

(利用する必要がなくなった場合等の利用停止及び第三者提供停止の請求)

第36条 当社は、本人から、当該本人が識別される保有個人データについて、次の各号のいずれかに該当するとして、当該保有個人データの利用停止等又は第三者への提供の停止の請求を受けた場合には、直ちに、当該請求に理由があるかの調査を行わなければならない。

- (1) 当該本人が識別される保有個人データを当社が利用する必要がなくなった場合
- (2) 当該本人が識別される保有個人データに係る漏えい等事案が生じた場合
- (3) その他当該本人が識別される保有個人データの取扱いにより当該本人の権利又は正当な利益が害されるおそれがある場合
- 2 当社は、前項の規定による保有個人データの利用停止等又は第三者への提供の停止の請求に理由があることが判明したときは、本人の権利利益の侵害を防止するために必要な限度で、遅滞なく、当該保有個人データの利用停止等又は第三者への提供の停止を行わなければならぬ。ただし、当該保有個人データの利用停止等又は第三者への提供の停止に多額の費用を要する場合その他の利用停止等又は第三者への提供の停止を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない
- 3 当社は、第1項の請求に係る保有個人データの全部又は一部について利用停止等を行ったとき若しくは利用停止等を行わない旨の決定をしたとき、又は第1項の請求に係る保有個人データの全部又は一部について第三者への提供を停止したとき若しくは第三者への提供を停止しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

第5章 苦情処理

(苦情の処理)

第37条 当社は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努める。

- 2 当社は、前項の目的を達成するために必要な体制の整備に努める。
- 3 第1項で定める個人情報の取扱いに関する苦情処理の担当者は、適宜、個人情報取扱責任者及び当社代表者に苦情の内容を報告するものとする。

第6章 その他

(罰則)

第38条 当社は、本規程に違反した従業員に対して就業規則に基づき処分を行い、その他の従業者に対しては、契約又は法令に照らして決定する。

附 則

第1条 本規程は、 年 月 日より実施する。

資料3 漏えい等事例

2014年
7月

○ ベネッセ顧客情報漏えい事件発覚【不正アクセス・刑事／損害賠償請求／委託先の監督・安全管理措置・従業者の監督】

【概要】

(株)ベネッセコーポレーション(ベネッセC)から顧客個人情報の統合・分析に使用するシステムの開発・運用・保守の業務委託をうけた(株)シンフォーム(ベネッセグループ)が、2012年4月にシステム開発をA社(グループ外)に再委託。A社からシンフォーム事業所(入退館管理有)に派遣されたSEのMが、シンフォームから貸与されたPCから複数回ベネッセCのデータベースにアクセスし(アカウントは提供された正規のアカウント)、「進研ゼミ」などの顧客情報約3504万件、約4858万人分を抽出して貸与PCに保存のうえ、貸与PCにUSB接続したMTP通信対応のスマートフォンに転送して不正取得(調査委員会報告、H30.12.27東地判)。

Mは名簿業者3社に顧客情報を売却して約400万円を得ており、顧客情報は最終的には500以上の業者に流出した(報道)。そのうち、名簿業者「セフティー」は2013年7月から2014年6月までの間、10数回にわたりMから計282万円で購入した顧客名簿を50社以上に転売して1600万円を売り上げたとみられる(警視庁発表)。

Mの動機は約170万円の借金。

名簿業者から約257万件分を購入したジャストシステムや約7万5000件分を購入したECCらがDM送付に利用した(両者とも後に利用停止)。金銭的被害の報告はない。

【漏えいした情報】

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、出産予定日、保護者の氏名など(東京高判R2.3.25)

【脆弱性】(調査委員会報告、H30.12.27東地判より)

クライアントPCとサーバ間の通信量が一定の閾値を超えた場合にシンフォームの担当部長にメール送信されるアラートシステムの対象にMのクライアントPCとサーバ間の通信が設定されておらず、Mによる不正行為に対してアラートシステムが機能しなかった。

社内規程で社内PCのデータを外部メディアに書き出すことが原則禁止され、運用上も書き出し制御システムが導入されていたが、クライアントPCのUSBポートは開放され、特定の新機種のスマートフォンへの書き出しに制御システムが機能しない状態であり(書き出し制御システムはMSC対応であったが、MのスマホはMTP通信対応で、MTP通信利用による情報漏えいリスクは情報セキュリティ専門家でもほとんど認識されていなかった)、Mがその事実に気づいた。

ベネッセグループでは、全体の情報セキュリティの統括責任者が明確でなく、統括的に管理する部署も存在せず、個人情報管理の責任部門も不明確で、実効性ある監査は実施されていなかった。

ベネッセCやシンフォームでも組織再編の結果、組織間で権限・責任の所在が不明確になる場合があった。

【会社の対応等】

6/26以降 ベネッセCのみに登録していた個人情報で、他社からDMやセールス電話が来ているとの問合せが急増

6/28 緊急対策本部設置(本部長はベネッセC社長)、調査会社を起用

6/30 経産省に報告・相談、所轄警察署に報告・相談、お客様問合せ窓口設置

7/4 調査会社報告により名簿業者を把握し名簿を入手。保有データと名簿をマッチングさせた結果、ベネッセCしか保有していないデータが含まれていることが判明

7/7 社内調査の結果、データベースから顧客情報が持ち出されていることが判明

7/8 漏えいが疑われる顧客名簿を取り扱っている名簿業者及び名簿を利用してDMや電話をしている企業に名簿の利用・販売の中止を求める内容証明郵便を発送

7/9 顧客情報の漏えいを発表、顧客へのお詫びの文書発表(7/10)、経産省が報告徴収を要請(7/10。報告書提出は7/17)、お詫びと対策状況に関する新聞広告(7/11)

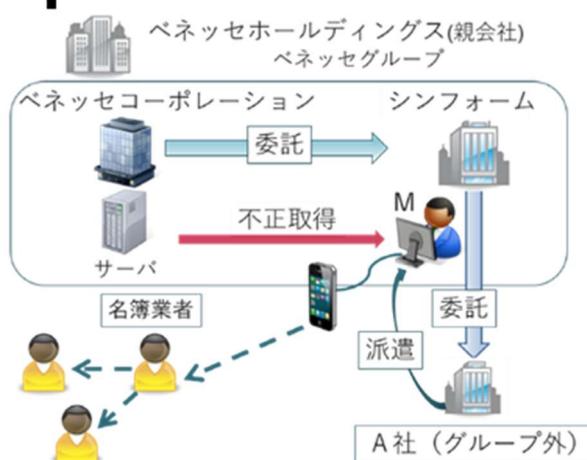
7/15 (株)ベネッセホールディングス(BHD)に事故調査委員会設置(弁護士、セキュリティ関連企業役員及びBHD役員ら計5名。メンバー決定は7/22)、警視庁に刑事告訴

7/17 Mを逮捕(2014/8/7起訴)(報道)

9/17 経産省に最終報告書提出

9/25 調査委員会報告

9/26 BHDに外部監視機関設置(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で構成) 経産省が個人情報保護法に基づき勧告



9月下旬 対象者にお詫びとして500円分の金券（楽天edy・amazonギフト券・nanaco・図書カードから選択）又は新たに設立した「ベネッセこども基金」への500円寄付の選択

【影響】

BHDの代表取締役副会長と取締役1名が管理監督責任を重く受け止め辞任（2014/7/31）

BHD発表の2014年第1四半期（4～6月期）決算で、特別損失を260億円計上（お客様へのお詫び200億、情報セキュリティ対応60億），最終損失が136億円と初めて赤字に転落。進研ゼミの会員数はピーク時約420万人から2015年4月には約271万人（報道）

JIPDECがベネッセCのプライバシーマーク付与取消し措置を決定（2014/11）。JIPDECはジャストシステムに対しては勧告措置（2014/10）

Mは不正競争防止法違反（営業秘密の複製、開示。同法21条1項）の容疑で逮捕・起訴され、懲役2年6月（実刑）及び罰金300万円（東京高判H.29.3.21）。

Mから顧客情報を購入して転売した名簿業者「セフティー」と同社社長は不正競争防止法違反（営業秘密の取得・開示）の被疑事実で書類送検（社長は営業秘密の認識を否認）（2015/3/30。報道）。

「被害者の会」「被害者弁護団」のもと、ベネッセC、シンフォーム、BHDに対する損害賠償請求の訴訟が第5次訴訟まで提起。

着手金・実費0円で成功報酬制。第1次訴訟は原告1人あたり5万5000円、総額9839万5000円を請求（原告1789名）、第2次訴訟は総額9630万5000円を請求（原告1751名）、第3次訴訟は総額2億7500万円を請求（原告5000名）、第4次訴訟は総額5604万5000円を請求（原告1019名）、第5次訴訟は総額6435万円を請求（原告1170名）（被害者の会HP）。この他にも、集団的訴訟や、弁護士等個人による訴訟提起もあり。

○ 東京高判R1.6.27（顧客2名がベネッセCとシンフォームに対して1名は3万円、もう1名は10万円の損害を請求して提訴し敗訴した東京地判と横浜地判の控訴審）

シンフォームにはスマホによる書き出し制御措置を講ずべき注意義務の違反、ベネッセCにはシンフォームに対する適切な監督をすべき注意義務の違反があり、共同不法行為が成立するが、原告らには慰謝料請求権を認め得るほどの精神的苦痛が生じたと認めることはできないとして請求棄却した一審判決を変更し、シンフォームとベネッセCに対し、共同不法行為に基づき1人あたり2000円の損害賠償（連帯責任）を命じた。

- ・ シンフォームについては、スマホによる書き出し制御措置を講ずべき注意義務違反の過失があるとして、固有の不法行為責任を認めた（再委託先の従業員Mとの実質的な指揮監督関係は認めず使用者責任は否定した）。
- ・ ベネッセCについては、委託先であるシンフォームに対しセキュリティソフトの適切な設定を行っているか否かを監督する注意義務違反の過失があるとして固有の不法行為責任を認めた。

損害については、漏えいした個人情報から何らかの重大なプライバシー情報が引き出されるとは想定しにくく、望まないDMが増えるかもしれないという危惧以上に何らかの実害が発生したとは認められない上、本件漏えいの発覚後にベネッセホールディングスが直ちに被害拡大防止措置を講じていること、ベネッセCも顧客の選択に応じて500円相当の金券を配布する慰謝の措置を講じていることなどから、1人あたりの損害額を2000円と認定し（慰謝料のみで弁護士費用は認めず）、シンフォームとベネッセCの共同不法行為責任（連帯責任）を認めた。

○ 東京高判R2.3.25（462人がベネッセCとシンフォームを被告として、漏えい当時成年の場合は1人あたり5万円、未成年の場合は1人あたり10万円、計約3590万円の損害を求めたが、ベネッセCの責任は否定された東京地判の控訴審）

シンフォームのMに対する使用者責任を認めつつベネッセCの不法行為責任は認めなかった一審判決を変更して、シンフォームとベネッセCに対し、共同不法行為に基づき1人あたり330円の損害賠償（連帯責任）を命じた。

- ・ シンフォームについては、セキュリティソフトのバージョンアップの際の取説や販売代理店からの説明等によってセキュリティソフトの設定変更によりデバイスの接続制御措置をとることが可能であったことを認識できたにもかかわらず設定を変更しなかったことについて、セキュリティソフトを適切な設定内容に変更する注意義務違反の過失があるとして、固有の不法行為責任を認めた（再委託先の従業員Mとの実質的な指揮監督関係は認めず使用者責任は否定した）。
- ・ ベネッセCについては、委託先であるシンフォームに対する適切な監督をすべき注意義務違反の過失があるとして固有の不法行為責任を認めた（ベネッセCとシンフォーム又はMとの実質的な指揮監督関係は認めずベネッセCの使用者責任は否定した）。
- ・ 損害については、漏えいした個人情報は出産予定日を除き人が社会生活を営む上で一定の範囲の他者に開示することが予定されている個人を識別するための情報又は個人に連絡をするために必要な情報もあるため、思想・信条、病歴、信用情報等とは異なり、個人の内面等に関わるような秘匿されるべき必要性が高い情報とはいえないことや、財産的損害その他の実害が生じたことがうかがわれないこと、本件漏えいの発覚後にベネッセホールディングスが直ちに被害拡大防止措置を講じていること、ベネッセCも顧客の選択に応

	<p>じて500円相当の謝罪品の交付を申し出るなどしていることなどから、1人あたりの損害額を3300円（慰謝料3000円、弁護士費用300円）と認定した。</p> <ul style="list-style-type: none"> ・そして、シンフォームとベネッセCの共同不法行為責任（連帯責任）を認めた。 <p>○ 東京地判R5.2.23（「被害者の会」による第3次訴訟を除く第1次から第5次訴訟までの判決）→ベネッセCが控訴し東京高裁で審理中（2023.10時点）</p> <p>シンフォームとベネッセCに対し、共同不法行為に基づき1人あたり3300円の損害賠償（連帯責任）を命じた（なお、被告ベネッセCが控訴した）。</p> <ul style="list-style-type: none"> ・シンフォームについては、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の違反の過失があったとして、固有の不法行為責任を認めた（再委託先の従業員Mとの実質的な指揮監督関係は認めず使用者責任は否定した）。 ・ベネッセCについては、委託先であるシンフォームに対する監督を怠った過失があるとして固有の不法行為責任を認めた（ベネッセCとシンフォーム又はMとの実質的な指揮監督関係は認めずベネッセCの使用者責任は否定した）。 ・損害については、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とし、慰謝料3000円、弁護士費用300円の合計3300円を損害と認定した。 ・そして、シンフォームとベネッセCの共同不法行為責任（連帯責任）を認めた。
2023年 6月	<p>○社労夢サーバのランサムウェア感染事件発覚【不正アクセス・安全管理措置】</p> <p>【概要】</p> <p>（株）エムケイシステムの「社労夢」（社労士業務支援システム）等を提供しているデータセンター上のサーバが不正アクセスを受け、ランサムウェア（感染したコンピュータのシステムへのアクセスを制限し、制限を解除するための身代金を要求するプログラム）が実行されてサーバ上のデータが暗号化され、暗号化されたデータへのアクセスができない状況となった。結果としてシステムが停止し、同社サービスの対象である約3,400ユーザーの大半に対して正常にサービスを提供できない状況となり、システムの提供を受ける社労士事務所が顧問先の給与計算等ができなくなる等の影響を受けた。</p> <p>同社が保有する顧客の個人情報が流出したおそれがあるが、情報流出は確認されていない（同社発表）。同社が預かっている顧客のマイナンバーも流出した可能性があると報道されたが、同マイナンバーは他の社労夢製品とは切り離した環境で高度な暗号化処理を施しており、本件の流出のおそれがある情報範囲には含まれていない（同社発表）。</p> <p>【漏えい等のおそれがあるデータ】※委託元企業の発表より（社労士事務所が顧問先企業からどのような業務を受諾しているかにより異なる）</p> <ul style="list-style-type: none"> ・同社サービスを利用している社労士事務所の顧問先企業の従業員・元従業員の氏名・住所、育児・介護休業給付金の申請にかかる情報、雇用保険取得・喪失の申請にかかる情報、労災保険の申請にかかる情報等 <p>【会社の対応等】</p> <p>6/5 同社データセンター上のサーバがダウンしたため、インフラ担当者がデータセンターへ直行して状況を確認するとともに調査を開始。画面上にランサムウェアらしき警告文を確認し、不正アクセスの可能性が発覚したため、関連するインターネット回線を切断。外部専門家も合流して調査を継続した結果、ランサムウェアによる第三者からの不正アクセスと断定するとともに、社労夢システムのサービス提供用サーバ全てが暗号化され動作しないことが判明した。</p> <p>同社は対策本部を設置するとともに、外部の情報セキュリティ会社へ対応を要請し、状況ヒアリングや原因把握の作業を実施（～6/7）</p> <p>6/6 大阪府警高度情報推進局サイバーセキュリティ対策課へ通報し事情聴取を実施し、今後の対応について助言を仰ぐ。</p> <p>「第三者によるランサムウェア感染被害のお知らせ」を発表（適時開示）</p> <p>6/7 外部専門家とデータセンターにおいてサーバの現地調査実施するとともに、データセンター内関連機器のログ保全を行い、感染経路調査を開始。</p> <p>6/8 個人情報保護委員会へ報告（速報）</p> <p>6/9 「第三者によるランサムウェア感染被害への対応状況のお知らせ」を発表（適時開示）</p> <p>同社はシステム復旧に向けた再構築を余儀なくされ、従来のデータセンター（IDC=インターネットデータセンター）と新環境（AWS=Amazon Web Services）の両面で構築作業を実施（7/下旬ころ完了）</p>

	(復旧状況) ・給与計算 給与計算を急ぐ必要がある社労士事務所のために「ネットde賃金WEB版（顧問先版）」を社労士事務所用に改修し、約2,800の社労士事務所ユーザーに暫定版リリースとして案内。暫定版は6/13以降、バックアップ領域からデータベースの移行が完了した社労士事務所から順次稼働し、6/15にネットde賃金WEB版提供用の全データベース移行が完了 ・社労夢（社労士業務支援システム） クラウドではなく社労士事務所のローカル環境で稼働するシステムの運用を開始し、6/16に申込みサイトを開設して順次メールにてアプリ・データを送付して運用スタート（6/19時点で申込み約2300件、提供済み約1400件） ・ネットde顧問（社労士事務所が顧問先に提供するWeb明細・勤怠管理のクラウドサービス） 6/21に新環境版をリリース 6/21 「第三者によるランサムウェア感染被害への対応状況のお知らせ（第2報）」を公表（適時開示） 影響を受けたユーザー（約3400ユーザーの大半）に対し、6月分請求を停止（7月分はサービスのリリースに伴う日割りでの請求） 6/30 一部サービスの再開（順次再開し、7月中に全サービスの提供を再開） 7/19 個人情報保護委員会へ確報を提出 「当社サーバへの不正アクセスに関する調査結果のご報告（第3報）」を公表（適時開示） ・フォレンジック調査（デジタル機器の記憶装置から証拠となるデータを抽出し、サーバや通信機器などに蓄積されたログ等の証跡情報から発生事象を明らかにする手段や技術）の結果の概要を記載 ・社労士事務所の顧問先等の従業員からの問い合わせについて、「個人情報に関する個人の方（本人）のお問い合わせ先」を公表 ・実施済みの再発防止策と対策予定を記載 【影響等】 ・システム復旧に当たり、新たにクラウド基盤でのサービスを提供するため、ランサムウェアに感染したデータセンター内の既存サーバを撤去 ・既存サーバの撤去費用、システム復旧・サービス再開に要した外部専門機関への調査委託費用、インフラ整備の再構築費用、セキュリティ強化費用などで、固定資産除却損約1億2600万円、システム障害対応費用1億約3800万円を計上 ・影響を受けたユーザー（約3400ユーザーの大半）に対し6月分請求を停止、7月分をサービスのリリースに伴う日割りでの請求としたことや、対象ユーザーの解約、新規受注減少などにより、営業利益・経常利益の大幅な減益の見込みと当期純利益が当初予想を大幅に下回る見通しとなり、年間配当予想を当初の8円から4円に修正（8/8発表） ・役員報酬を減額（代表取締役は月間報酬の30%を減額、常勤取締役は月間報酬の10%を減額、常勤監査役は月間5%を自主返上）。
--	---