特別解説

応用一般

ベネッセ個人情報漏洩事件

上原哲太郎（立命館大学）

事実関係

通信教育などで知られる（株）ベネッセコーポレーション（以下ベネッセ）から子どもの名簿を中心とする個人情報が流出した事件は，マスコミにも大きく取り上げられた．我が国で発生する個人情報流出事件は報道されるだけでも年数千件に及ぶが，この事件は過去発生した個人情報漏洩事件（紛失ではなく）の中で最大となる約 3,000 万件分の漏洩となったこと，またその漏洩された本人に被害が及ぶような悪用が明白であったことから特に大きく報じられることとなった．本事件はその規模の大きさだけではなく，その内容についてもいくつか特筆すべき点があるので，ここにまとめておく．

本件の事実関係はおよそ以下の通りである．2014 年 6 月下旬ごろ，ベネッセと競合する通信教育事業を行う企業から，ダイレクトメールがベネッセの顧客宛に届きはじめた．それを期にベネッセにおいて社内調査が行われた結果，特定の社内データベースからの顧客名簿の持ち出しが明らかになった．

同社の発表[1]や各種報道によると，同社の情報システムの開発や運用はグループ企業である（株）シンフォームに委託されていたが，シンフォームはさらに複数の企業に業務委託をしており，開発や管理運用が多重の下請け構造の中にあったようである．その中で，あるシステムの開発および管理運用受託企業の社員（その後解雇されたため以下，元社員と表す）が，顧客情報データベースへのアクセス権限を悪用して業務中に複数回に渡り顧客情報（一部アンケートに応じた人など，顧客ではない人の情報も含まれる）を持ち出し，ダイレクトメール用の名簿などを扱う事業者に売却した．持ち出された名簿は複数の名簿業者間で転売されたあと，ベネッセの競合事業者の手に渡りダイレクトメールに使用されたことで，当該顧客情報の漏洩が発覚した（図 -1）．

事故原因となった脆弱性

ではそもそもなぜ顧客情報の持ち出しが可能だったのか．報道などを総合すると同社の情報システムはかなり厳しい管理下に置かれていたように思われる．システムは外部のセキュリティ監視サービス会社により 24 時間監視を受けていたため，外部からの攻撃で漏えいしたものではないことが早期に判断されたとされる．さらに，当該データベースへのアクセスもログが保管されており，それが実際に顧客情報を持ち出した元社員を速やかに特定するために役立ったようである．加えて，データの持ち出しを防ぐため，各端末の USB ポートには USB メモリなどのストレージが接続されてもデータが書き出せないようなシステムが導入されていた．しかし，このデータ漏洩防止策が不完全であったことが今回の事件に繋がっている．

元社員は作業中に私物のスマートフォンを端末の USB に接続し充電していたが，その際にスマートフォンが端末により認識され，ここにデータが書き出しできることに気づいたとされる．そこでこれを利用して顧客情報データベースの内容を書き出してはスマートフォンに転送し，持ち出して転売していたと見られる．一般に Windows では，USB に接続される外部記憶媒体は USB マスストレージクラスと呼ばれるドライバを介してアクセスされるので，

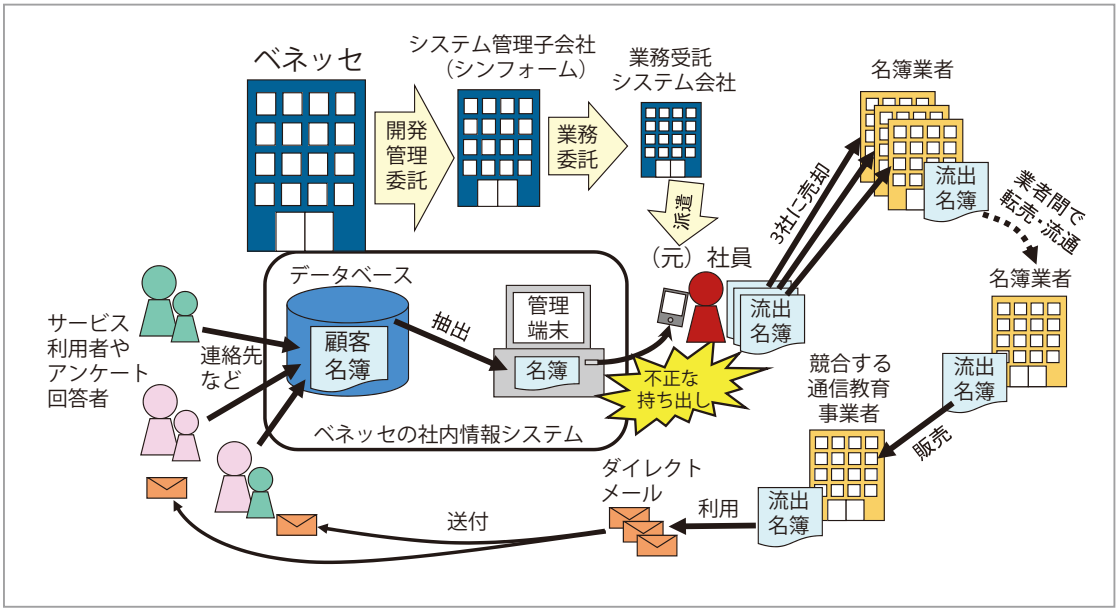

図 -1
ベネッセから流出した名簿の流れ

このドライバの機能を制限することで USB メモリ等への書き出し禁止が実現できる．しかし USB に接続されるデバイスは多岐にわたり，USB マスストレージクラス以外でもファイルの転送が可能な接続方法が存在する．たとえば，デジタルカメラ等が接続された際に画像を転送するために用いられる PTP（Picture Transfer Protocol）と呼ばれるプロトコルや，この PTP を拡張し，より汎用性のあるファイル転送を可能にした MTP（Media Transfer Protocol）があり，最近の Android スマートフォンはこれらのプロトコルに対応している．MTP は元々画像や音楽などのメディアファイルの転送を意図したものだが，Windows における実装では通常の外部記憶と同様に任意のファイルの転送に利用できる．ほかに iPhone などの iOS を搭載したスマートフォンやタブレットも独自プロトコルによってパソコンとの間でファイル転送を行っている．外部記憶媒体と同様に利用できるプロトコルすべてに対するデータ書き出しを禁止するためには，これらに個別に対応する必要があるが，外部記憶装置へのデータ書き出しを禁止する機能を謳う製品には，これらすべてに対応しきれていないものがある．ベネッセの導入していたシステムも，このような例外的なデータ転送方法への対応漏れがあった模様である．

事件の背景

このように，今回の情報漏えいの直接的な原因は，このシステムの脆弱性を突かれたことにあるが，もう少し俯瞰してみると，以下のような背景が指摘できるだろう．

前述したようにベネッセの情報システムのデザインは比較的レベルが高いものであったが，運用にはいくつかの問題があったように思われる．たとえば，端末管理システムが導入されていたのは明らかであるのでシステムには端末に USB 機器の接続が行われた際のログが残っているはずであるが，これに十分な注意が払われていなかったのではないか．その結果，重要なデータを扱うシステムの運用現場に私物スマートフォンが持ち込まれ，充電のために接続されている状況が看過されていたと思われる．さらに，データベースへのアクセスログが取られていたことは明らかになっているが，これが定期的な監査を受けていなかったと思われる．今回の情報漏洩は 2014 年 1 月には始まっていたと報道されているため，半年以上ログの監査が行われていなかったと考えられる．また，データベースから大量のデータを抽出する操作が自由に行える環境だったと思われること，スマートフォンや MTP の普及といった環境の変化に対応が遅れ，前述のようなシステムの脆弱性が見過ごさ

れてきたことも運用体制の不備に挙げられるだろう．

社会的背景としては，個人情報保護法が完全施行された 2005 年以来，ダイレクトメールなどに利用できる名簿の入手は困難になってきたが，とりわけ 2005 年以降に産まれた子どもの名簿を取り扱うことが困難になっていたことが挙げられる．ベネッセは街頭のアンケートなどを通じて子どもの名簿を整備してきており，その名簿は貴重な情報資産となっているため名簿業者に高値で売れることに，元社員が気づいたことが事件を誘発した．元社員が多重の下請け構造の中にあって，元請け企業へのロイヤリティが希薄だったと考えられることも事件の要因と思われる．これは，過去の大規模な情報漏洩事件，たとえば 1999 年の宇治市基本台帳漏洩事件や 2007 年の大手印刷会社における個人情報漏洩事件が，いずれもシステムの開発や管理が下請け構造下にあった中で発生したことと似た構造にある．

なお，これまでの個人情報漏洩事件と今回が刑事事件として大きく異なるのは，はじめてこの種の事件に不正競争防止法が適用されていることである．民間における個人情報保護法には漏洩に対する直罰が規定されていないため，これまで記憶媒体に対する窃盗罪やシステムに対する不正アクセス禁止法違反などで立件されてきたが，今回のような正規のアクセス権限を持つ内部犯しかも物理的媒体の窃盗を伴わない情報漏洩の場合には立件が困難だった．それがこの事件では，持ち出された名簿がベネッセの営業上の秘密と認められたことと，2009 年の同法改正以降，営業秘密の漏洩罪が「競合関係にある者」による直接の犯行でなくとも適用されることになったことで，同罪での立件が可能だった[2]．同法の改正はいわゆる産業スパイの取り締まり強化を目的としたものであったが，このような個人情報漏洩事件にも適用可能であることが示されたのは大きな意味がある．

残された課題

この事件が残した課題としては以下のようなものが挙げられるだろう．情報システムの運用にあたっては，重要な情報資産へのアクセスログを残すだけでなく，それを定期的に監査することが重要である．さらには，業務の従事者にその管理ログを残して監査していることを強く印象づけておくことが，犯罪・不正の事前抑止と早期発見に有効であることを，改めて啓蒙する必要がある．加えて，この種の重要なシステムの運用に関して，現在のような多重下請け構造下で技術者を管理監督することの限界も指摘できるだろう．なお，本事件を受けてベネッセは，重要な個人情報を扱うシステム専門の子会社を，大手情報セキュリティ事業者と合弁で設立し，その子会社にシステム開発運用を委託するとしていることは興味深い[1]．

社会的には，今回話題になった名簿業者を今後どう取り扱うべきかが大きな課題であろう．現行の個人情報保護法は各事業者に対し，個人情報の第三者提供に対して本人の同意を必要とするという制約を設けているが，名簿業者の個人情報はそもそも本人の知り得ない間に流通し，違法であっても実効ある制限ができない．現行の個人情報保護法でも，これらの業者からの名簿の入手は本人同意がなければ適正な個人情報の入手とはいえないとの指摘もあり，今後何らかの規制につながる可能性もある．ちょうど現在進められている個人情報保護法の改正では，ビッグデータ時代を迎えて新産業の育成を目指し，個人情報の利活用をどのように認めていくべきかという議論が主にされてきたが，本事件が個人情報流通に対してさらなる規制を求める議論を喚起することが予想される．個人情報の保護と利活用に関するバランスのとれた法制度に向けてどのような議論が行われるか，今後の動向が注目される．

参考文献

1) （株）ベネッセホールディングス「お客様情報の漏えいに関するご報告と対応について」，2014 年 9 月 10 日．
2) 須川賢洋：営業秘密について考える，デジタル・フォレンジック研究会，第 322 号コラム，2014 年 8 月．

（2014 年 9 月 11 日受付）

上原哲太郎（正会員） uehara@cs.ritsumei.ac.jp

立命館大学情報理工学部情報システム学科教授（サイバーセキュリティ）．1995 年京都大学大学院工学研究科情報工学専攻博士後期課程研究指導認定退学．和歌山大，京大，総務省を経て 2013 年より現職．京都大学博士（工学）．