〔論　説〕

ベネッセ顧客情報漏えい事件の事例研究

樋　口　晴　彦

キーワード: 組織不祥事，リスク管理，情報セキュリティ，情報漏えい，アウトソーシング

はじめに

本稿は，ベネッセグループの中核企業である株式会社ベネッセコーポレーション（以下，会社名では「株式会社」を省略する）が保有する顧客等の個人情報（以下，「顧客情報」とする）が，内部不正によって大規模に漏えいした事件（2014年7月発覚）に関する事例研究である。

本研究では，内部不正を防止あるいは早期に発見できなかった原因として，書出し制御システムの不備，私物機器持ち込みの放任，アクセス範囲の未区分，アクセスログの未確認，アラートシステムの未設定，不明確なセキュリティ責任者及び担当部署の計6件のセキュリティ対策上の問題点を抽出するとともに，その背景の一つとして，情報活用優先の経営方針について指摘した。

本事件を誘発した原因メカニズムとしては，業務委託先に対する管理を懈怠し，基本的なセキュリティ対策さえ実施していなかった問題に関して「委託側の責任感喪失のリスク」，経営者側のIT業務に関する理解が不足し，セキュリティ対策の不備を認識していなかった問題に関して「傍流事業の特殊性による組織不祥事リスク」の2類型を抽出した。

1. 事件の概要[(1)]

ベネッセホールディングス（以下，「ベネッセHD」とする）は，通信教育や出版を主な事業とする企業であり，東京証券取引所第1部に上場している。同社の2014年3月期の連結経営指標は，売上高466,399百万円，経常利益35,216百万円，当期純利益19,930百万円であった。

ベネッセグループの中では，持株会社のベネッセHDが経営方針の策定や経営管理を行い，その100%子会社であるベネッセコーポレーション（以下，「ベネッセコーポ」とする）が事業面の中核である。事業分野としては，「進研ゼミ」や「こどもちゃれんじ」などの通信教育講座（会員数365万人）を中心とする国内教育事業が最も大きく，2014年3月期の売上高は251,762百万円（全体の54.0%）であった。

2014年6月27日，顧客からの問い合わせ[(2)]によって，ベネッセコーポが管理する顧客情

(1)　ベネッセHDでは，「個人情報漏えい事故調査委員会」（以下，「調査委員会」とする）を設置し，本事件の事実調査，原因究明及び再発防止策の策定に当たらせた。本稿における事実関係の認定は，主として同委員会の調査報告書（以下，「調査委員会（2014）」とする）に依拠している。

(2)　「ベネッセのみに登録していた個人情報で，他社からダイレクトメールやセールス電話が来ている。ベネッセ

報[3]が社外に漏えいしている疑いが浮上した。社内調査の結果，データベースから情報が不正に持ち出されていた事実が判明し，システムエンジニアのAが不正競争防止法違反（営業秘密複製）容疑で逮捕・起訴された。

流出した顧客情報の延べ件数は2億1,639万件であるが，同一人物の情報が複数回計上されているケースがあるため，ベネッセコーポで名寄せ作業を実施した結果，3,504万件（4,858万人分）と推定されている[4]。この事件を受けて，ベネッセHDでは取締役2人[5]が引責辞職するとともに，2015年3月期の第1四半期報告書（2014年4～6月）では，事件処理に関連して260億円の特別損失を計上した[6]。

また，経済産業省は，個人情報保護法違反（個人情報の安全管理措置義務違反（法第20条）及び委託先の管理監督義務違反（法第22条））が認められたとして，2014年9月にベネッセコーポに対し，個人情報の漏えいの再発防止に向けて，業務委託先も含めた個人情報の保護に関する実施体制の明確化及び情報セキュリティ対策の具体化を行うように勧告した。

2. 犯行の態様

ベネッセコーポでは，システムの開発・運用をベネッセHDの100%子会社であるシンフォームに任せていた。シンフォームでは同業務の一部を他の企業に委託し，委託先企業はさらに別の企業に再委託していた。Aは，その再委託先企業の社員であり，2012年4月からシンフォームの東京支社多摩事業所で働いていた。

2013年7月，Aは，執務室内で業務用のクライアントPC[7]に私物のスマートフォンを充電する目的で接続したところ，PC内のデータを外部記録媒体に書き出せないようにする「書出し制御システム」が機能せず，データをスマートフォンにコピーできることに気が付いた。そこでAは，データベース内の顧客情報をクライアントPC内にコピーした上で，当該PCからUSBケーブルを通じて情報をスマートフォンに転送し，その内部メモリに保存

から個人情報が漏えいしているのではないか」との問い合わせであった（ベネッセHDのニュースリリース（2014年7月9日付））。

(3) ベネッセコーポと契約を結んだ顧客だけでなく，同社が商業施設でイベントを開催したときなどに，当人の同意を得て住所氏名などの情報を取得した者を含んでいる。
「ベネッセが出産・育児関連の共同事業を全国の自治体や企業に持ちかけると，次々と話がまとまる。そこに，懸賞応募や資料請求など，個人情報を集める仕掛けを組み込んだ。通信教育講座「こどもちゃれんじ」のキャラクター「しまじろう」をはじめ，ベネッセの育児・教育関連コンテンツへの信頼は絶大だった」（日経ビジネス2014年9月22日号「ベネッセ，覆水の始末　②慢心」26頁）。

(4) ベネッセHDのニュースリリース（2014年9月10日付）によると，漏えいした情報の項目は，サービス登録者の名前・性別・生年月日，同時に登録した保護者または子供の名前・性別・生年月日・続柄，郵便番号，住所，電話番号，FAX番号，出産予定日，メールアドレスである。なお，クレジットカード番号の漏えいは確認されていない。

(5) ベネッセHD代表取締役副会長（犯行時のベネッセHD代表取締役社長）及び同取締役兼CIO（犯行時のベネッセコーポ代表取締役社長）の2人。

(6) 特別損失の内訳は「お客様へのお詫び」（1人500円の金券を配布）に200億円，「お客様へのお詫び文書の発送費用，及びお客様からのお問い合わせ対応費用，並びに個人情報漏えいに対する調査・情報セキュリティ対策等に係る費用」に60億円とされた。

(7) データベースへのアクセスを許可されたPCのこと。

する形で外部に持ち出した。

Aは，月1～2回の頻度で顧客情報を持ち出し，名簿業者3社に約250万円（合計額）で売却していた。新聞報道によると，Aの月収は約38万円であったが，パチンコや競馬で浪費したことに加えて，家族の入院が重なるなどしたことで，消費者金融などに約170万円の借金があったとされる[8]。

Aから顧客情報を入手した名簿業者は，他の名簿業者や企業にそれを販売した。その販売先の一つがジャストシステム[9]であり，2014年5月に約257万件の名簿を購入して，同6月に同社が運営する「スマイルゼミ」（小中学生向きの通信教育）のダイレクトメールを発送していた[10]。

3. 情報漏えい事件に関する調査状況

日本国内での内部不正による情報漏えい事件に関する調査状況は，以下のとおりである。

3.1 日本ネットワークセキュリティ協会の調査

NPO日本ネットワークセキュリティ協会（以下，「JNSA」とする）の「セキュリティ被害調査ワーキンググループ」と情報セキュリティ大学院大学は，2013年中に報道された個人情報漏えいインシデント（事件・事故）を調査分析し，『2013年　情報セキュリティインシデントに関する調査報告書　―個人情報漏えい編―　第1.1版』を発表した。

それによると，2013年中のインシデント件数は1,388件，漏えい人数は925万人分，想定損害賠償総額は1,438億円であった。件数別の原因上位は，ケアレスミスなどの「誤操作」（34.9%），誤廃棄などの「管理ミス」（32.3%），「紛失・置き忘れ」（14.3%）であるが，漏えい人数別の原因上位は，「不正アクセス」（78.7%），「管理ミス」（9.2%），「紛失・置き忘れ」（6.1%）であった。

「内部犯罪・内部不正行為」による漏えい事件は，2013年には14件（1.0%）と少なく，漏えい人数の比率は0.004%にすぎない。しかし，過去10年間の調査結果を見ると，件数はやはり少ないものの，漏えい人数の比率が非常に高くなっている年が認められる（表1）。これは，以下のように1件の漏えい人数が極めて多いケースが存在するためである。

・（2006年）　漏えい人数400万人のインシデントが2件発生
・（2007年）　同863万人のインシデントが発生
・（2009年）　同148万人のインシデントが発生

---

(8)　読売新聞2014年7月19日夕刊。

(9)　ソフトウェアの開発・販売を主な事業とする企業で，東京証券取引所第1部に上場している。同社の2014年3月期の連結売上高は16,936百万円であった。

(10)　この件についてジャストシステムのニュースリリース（2014年7月11日付）は，「ベネッセコーポレーションから流出した情報であると認識したうえでこれを利用したという事実は一切ございません」と弁明する一方で，「（データの）購入において，データの入手経路を確認しながら，最終的にはデータの出所が明らかになっていない状況で契約に至り，購入していたことが判明致しました」として，情報の出所を確認せずに購入したことを認めた。ちなみに同社は，事件発覚後に，企業の道義的責任として，問題のデータをすべて消去したとされる。

表1　内部犯罪・内部不正行為による漏えい事件の経年変化

	件　数	漏えい人数の全体比
2004年	29件	15.8%
2005年	14件	10.2%
2006年	22件	36.0%
2007年	8件	28.3%
2008年	19件	4.4%
2009年	16件	29.1%
2010年	9件	8.4%
2011年	26件	7.1%
2012年	30件	1.2%
2013年	14件	0.004%

（JNSAの各年の調査報告書に基づき筆者作成）

3.2 経済産業省の調査

経済産業省は，2012年に企業を対象（回答企業3,011社）に営業秘密の管理実態及び営業秘密の流出実態について調査し，『「営業秘密の管理実態に関するアンケート」調査結果』を発表した。

それによると，回答企業の13.5%が過去5年間に営業秘密の漏えいを経験（「おそらく情報の流出があった」との回答を含む）している。流出した情報の種類は，「顧客情報，個人情報」が82.5%，「経営戦略に関する情報」が38.5%，「製造に関するノウハウ」が34.4%，「サービス提供のノウハウ」が28.8%の順であった。

営業秘密の漏えいがなかったと回答した企業に対し，その要因として大きいものについて回答を求めたところ，「データ等の持ち出し制限を行ったこと」が28.0%，「情報の管理方針等を整備していること」が26.8%，「秘密保持契約を締結していること」が26.0%，「営業秘密侵害防止の教育，管理方針等の周知徹底を行っている」が18.1%，「データ等の暗号化・アクセス制限を行ったこと」が17.2%の順であった。

また，営業秘密の漏えいを経験した企業が，その再発防止のために強化または新たに導入した対策について回答を求めたところ，「営業秘密侵害防止の教育，管理方針等の周知徹底を行った」が38.7%，「データ等の持ち出し制限を行った」が29.0%，「情報の管理方針等を整備した」が28.0%，「データ等の暗号化・アクセス制限を行った」が23.1%，「秘密保持契約を締結するようになった」が18.3%の順であった。

3.3 社会安全研究財団の調査

財団法人社会安全研究財団の「情報セキュリティにおける人的脅威対策に関する調査研究委員会」は，内部犯行による情報漏えい事件について調査し，2010年に『情報セキュリティにおける人的脅威対策に関する調査研究報告書』を発表した。

この研究では，2007年から2009年6月までに検挙された30事例を調査対象としたが，そのうち情報流出Ⅰ（換金を目的とした道具的な犯行）は8事例であった。情報流出Ⅰの特徴的な傾向は以下のとおりであるが，本事件と符合するものが多い。

・（個人的・人格的特質）「男性」「大卒」「転職経験者」「相対的に高いIT技術を有する」「多額の遊興費を要する趣味嗜好」「多額の住宅ローンがある又は住宅ローン以外の借金がある」など。
・（環境要因）「システム管理やHP管理の担当者」「他者による業務チェックを受けない又は他に詳しい者がいない」「特に職場への不満はない」など。
・（犯行状況）「生活費を捻出するために情報を換金」「顧客情報を狙う」「犯行後もそのまま勤務」など。

さらに，情報流出Ⅰの典型例として，「個人的な資質としては，比較的高い学歴を有し，IT技術についても，システム管理やHP管理などある程度の技術力を有している。企業の文化や風土としては，少人数な組織で，ワンマンな経営者という独特の文化を有している。こうした環境の中，組織の経営にとって重要な業務に位置づけられるIT業務を犯行者が独占して取り組んでいる。他にIT業務に詳しい者がいないために，犯行者の専門性，非代替性は高いものとなっている」（社会安全研究財団（2010），62頁）と説明している。

3.4 情報処理推進機構の調査とガイドライン

独立行政法人情報処理推進機構は，社員（回答者3,000人）及び経営者・システム管理者（回答者110人）を対象に内部不正に関する意識調査を実施し，2012年に『組織内部者の不正行為によるインシデント調査　―調査報告書―』を発表した。同調査では，内部不正対策により犯行を抑止することが可能とした上で，以下の対策ポイントを提示した。

・「社員向けアンケート調査の結果から多くの人の犯行への気持ちを低下させうることが期待できる対策は，「社内システムの操作の証拠が残ること」であった。そのため，社内システムの操作の証拠が残す対策を導入検討することが内部不正の抑止に対して重要であるとともに，対策を行なっている事実を周知すること（定期的に証拠の確認を行ったことを周知する）が内部不正の抑止対策を検討するうえで重要である」（情報処理推進機構（2012），66頁）
・「社内システムの操作の証跡を確実に実施するためには，内部不正者を特定すること，及び内部不正の対象となる情報へのアクセスを管理する必要があり，重要情報を扱う「システムのアカウントの適切な管理」，「アクセス権限の適切な設定」なども重要である」（前同）

以上の調査結果を踏まえて，情報処理推進機構は，内部不正対策を効果的に実施できるようにするために，2013年に『組織における内部不正防止ガイドライン』（以下，「情報処理推進機構（2013）」とする）を発表した。その中で，本事件に関連する対策項目は，以下のとおりである。

・対策4（2）総括責任者の任命と組織横断的な体制構築
・対策4（3）情報の格付け区分
・対策4（5）利用者のアクセス管理
・対策4（8）重要情報取扱領域の物理的な保護及び入退管理
・対策4（9）情報機器及び記録媒体の持出管理及び監視
・対策4（11）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
・対策4（12）無許可ソフトのインストール禁止と外部サービスの利用制限
・対策4（16）業務委託時のセキュリティ対策の確認

・対策4（17）ログ・証跡の記録と保存及び定期的な確認
・対策4（18）システム管理者のログ・証跡の確認
・対策4（19）教育による内部不正対策の周知徹底
・対策4（30）内部不正対策の定期的及び不定期的な確認及び監査

4. セキュリティ対策上の問題点

情報処理推進機構（2013）に列挙された対策項目は，決して目新しい内容ではなく，多くの企業で既に実践されている対策を取りまとめたものであり，言わば「情報セキュリティの常識」と位置付けられる。これらの対策項目と照合する形で，ベネッセグループの情報セキュリティについて検証すると，以下の諸点では適切な対策が実施されていた。

・ベネッセコーポのデータベースは専用回線でシンフォームの執務室に接続され，シンフォームでは，入館許可証を発行して執務室の入退管理を実施するとともに，その出入口には監視カメラを設置していた（対策4（8）関係）。
・データベースにアクセスできるクライアントPCについては，ワイヤーロックによる持出防止措置が取られていた（対策4（9）関係）。
・クライアントPCについては，ソフトのインストールの制御，外部サービスへの接続禁止などの対策を講じていた（対策4（12）関係）。
・ネットワークの使用状況についてはログが保存されていた（対策4（17）関係）。
・委託業務に従事する者には，情報セキュリティ研修を毎年受講させていた（対策4（19）関係）。

その一方で，以下の6件のセキュリティ対策上の問題点が存在したため，Aによる内部不正を防止あるいは早期に発見できなかったものである。

4.1 書出し制御システムの不備

情報処理推進機構（2013）は，「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で，個人の情報機器及び記録媒体による情報漏えいの対策を講じる」と解説している（対策4（11））。

シンフォームでは，クライアントPC内のデータを外部記録媒体に書き出せないようにするための「書出し制御システム」を整備していた。しかし，Androidを搭載するスマートフォンの新機種では，ファイル転送規格がMTPに変更されていたため，「書出し制御システム」が機能しない状態となっていた[(11)]。この問題は，2013年の段階で一部のセキュリティ技術者の間では認識されていたが，シンフォーム側の知識不足により未対応となって

（11）「Android搭載スマホは，2011年10月発表のバージョン4.0から，「MTP（Media Transfer Protocol）」と呼ぶファイル転送規格に本格対応した。MTPは，Windows OSが「WPD（Windows Portable Devices）と認識するデジタルカメラなどのデバイスを主な対象に，米マイクロソフトが策定した規格だ。PCがファイルを制御する「USBマスストレージ」と異なり，デバイス側でファイルを制御するため，（中略）本来はWPDも含めて，外部デバイスへのコピーを禁止する必要がある。しかしMTP規格を考慮せず，単にUSBマスストレージのみ使用禁止にすると，今回のような「穴」が生じる恐れがある」（日経コンピュータ2014年8月7日号「ベネッセホールディングス　空前「2300万件漏洩」の真因」57頁）。

いたと推察される[12]。

また，データを外部記録媒体に書き出せないようにするには，クライアントPCを外部記録媒体に接続できない仕様にしたり，データをクライアントPC内にダウンロードできないようにシンクライアント方式にしたりするハード面の対策も非常に有効であるが，シンフォームでは実施していなかった[13]。

なお，情報処理推進機構（2013）は，本事件を受けて，2014年9月に内容を一部改定した際に，「各部門責任者，担当者等は，情報通信技術の進歩や新たな脅威の出現，新しい法律の施行など技術的・社会的な変化に対応して，必要な知識の収集，能力の高度化を図ることができるよう，組織外の情報源からの情報収集や研修等に継続的に取り組むようにします」（対策4（19））及び「内部不正の対策は，情報通信技術の進歩や，新たな脅威の出現，新しい法律の施行，など技術的・社会的な状況によっても見直す必要があります。継続して，見直し，改善を図ります」（対策4（30））と解説を追加した（傍点筆者）。

4.2　私物機器持ち込みの放任

情報処理推進機構（2013）は，重要情報の外部への持出しや送信を防止するために，重要情報を取扱う領域への個人のモバイル機器や外部記録媒体の持込みを制限することを定めている（対策4（11））。

シンフォームの社内規定では，私物PCの持込みを制限していたが，スマートフォンの持ち込みについては制限していなかったとされる[14]。実務的にも，執務室への入退に当たって，所持品の確認などの持込み防止対策は取られていなかった[15]。

4.3 アクセス範囲の未区分

情報処理推進機構（2013）は，重要度に則して情報を格付け区分し，その区分に応じて取扱者を限定するとともに，情報へのアクセス権を適切に付与すること及びアクセス権を定期的に見直すことを求めている（対策4（3）・（5））。

Aは，システムの保守・管理業務を担当していたが，事業部門からの依頼に基づきマー

（12）「デバイス制御ソフトの対応も，メーカーによって異なっていた。2009年にWPDの制御機能を実装していたソフトがある一方，2013年まで対応できていないソフトもあった。マイクロソフト製品のセキュリティに詳しい濱本常義氏によれば，この問題は2013年ごろからセキュリティ技術者の間で話題になっていたという」（日経コンピュータ2014年8月7日号「ベネッセホールディングス　空前「2300万件漏洩」の真因」57頁）。

（13）事件後の対策として，ベネッセでは，シンクライアント方式を導入するとともに，クライアントPCに業務データが保存されていないかどうかを定期的に確認することとした。

（14）「（本事件を受けてベネッセHDでは，）物理的な対策としては，顧客DBを扱う執務スペースへの私物の持ち込みを禁止した。これまで私物PCの持ち込みは制限していたが，スマートフォンの持ち込みは制限していなかったという。同社は執務スペースに，監視カメラや金属探知機を設けることで，電子機器の持ち込みを防ぐ考えだ」（日経コンピュータ2014年10月2日号「4800万人の情報漏洩でベネッセが決断」6-7頁）。
「物理的監視におけるベネッセの対応で，セキュリティ技術者の誰もが首をひねるのが「容疑者が，顧客DBを扱う部屋に私物のスマホを持ちこめていた」という点だ。スマホのカメラを使い名簿リストを直接撮影するか，データをQRコードに変換して連続撮影すれば，データの持ち出しが可能になる」（日経コンピュータ2014年8月7日号「ベネッセホールディングス　空前「2300万件漏洩」の真因」58頁）。

（15）事件後の対策として，ベネッセでは，「執務スペースへの私物である電子機器，記録媒体の持込み禁止，監視カメラの導入」（ベネッセHDニュースリリース（2014年9月10日付））を実施した。

ケティング用に顧客情報を分析することも業務としていたため，データベースに対するアクセス権を付与されていた[16]。ところが問題のデータベースでは，情報の細分化や抽象化がなされておらず，アクセス範囲を区分していなかったために，Aは顧客情報の全てにアクセスすることが可能だった[17]。

4.4 アクセスログの未確認

情報処理推進機構（2013）は，「契約期間中，委託先が契約通りにセキュリティ対策を実施していることを確認しないと，委託先等の不備による情報漏えい等を防止できない可能性があります」と解説している（対策4（16））。さらに，重要情報へのアクセス履歴や操作履歴のログを保存して定期的に確認するとともに，大きな権限を持つシステム管理者についても，定期的に他者がログを確認することを求めている（対策4（17）・（18））。

シンフォームでは，クライアントPCからベネッセコーポのサーバーにアクセスした場合，自動的にアクセスログ及び通信ログが記録される設定にしていた。しかし，これらのログについて定期的にモニタリングする体制が存在しなかったため，Aの異常な操作履歴を把握できなかった[18]。

4.5 アラートシステムの未設定

情報処理推進機構（2013）は，「重要情報を格納している情報システムでは，時間及びアクセス数・量等のアクセス条件による制御を行うことが望まれます。（中略）アクセス数・量であれば重要情報を一括してダウンロードすると上司等に通知されるようにします」と解説している（対策4（5））。

シンフォームでは，情報漏えいを防止する目的で，クライアントPCとサーバーの間の通信量が一定の閾値を超えた場合に，担当部長に対してメールでアラートが送信される「アラートシステム」を整備していた。しかし，このアラート機能が未設定であったため，Aの行為に対してアラートが発信されなかった[19]。

4.6 不明確なセキュリティ責任者及び担当部署

情報処理推進機構（2013）は，「総括責任者は，組織横断的な管理体制や関連部門の役割を具体化，明文化し，その役割を徹底させます。責任部門は総括責任者と共に組織全体で

（16）「容疑者はデータベースの保守・管理に加えて，事業部の依頼に応じてこれらの情報をマーケティング目的で分析する役割まで担っていた。業務委託先の社員でありながら大量の個人情報にアクセスできる権限まで持っていたのは，そのためだ」（日経ビジネス2014年9月29日号「ベネッセ，覆水の始末　③陥穽」26頁）。
　なお，シンフォームのITソリューション部には「顧客分析課」という部署が存在した事実が認められ，Aがマーケティング用に顧客情報を分析していた件は，同社では決して特殊なことではなかったと思量される。

（17）「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」（調査委員会（2014），6頁）。

（18）事件後の対策として，シンフォームにセキュリティ監査部を新設し，定期的にログ監査を行わせることにした。

（19）「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，A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」（調査委員会（2014），5頁）。

の内部不正対策の実施策と実施体制を構築します」と解説している（対策4（2））。

ベネッセグループでは，情報の戦略的活用については体制を構築[20]していたが，情報セキュリティについては，「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」（調査委員会（2014），13頁）とされる。また，グループ内でシステムの開発・運用を担当していたシンフォームが，情報セキュリティ面でどのような権限を有しているかも明確でなかった[21][22]。

4.7 小括

ベネッセグループは大量の顧客情報を保有していた上に，それが競争長所の源泉であることも十分に認識していた[23]。それにもかかわらず，同グループの情報セキュリティは前述したとおりの状況であり，「情報セキュリティの常識」である情報処理推進機構（2013）と照合すると，劣悪であったと断じざるを得ない。

6件の問題点のうち4.1については，書出し制御システムを導入していたが，新たに生起したセキュリティ上の課題に関して知識が不足していたために，未対応となっていたものである。その一方で，他の5件については，IT業務の専門知識を有している者であれば，「情報セキュリティの常識」に違背していることを容易に認識できたはずである。そこで，これらの問題点がどうして放置されていたのか検討する必要がある。

4.2の「私物機器持ち込みの放任」及び4.4の「アクセスログの未確認」については，業務委託先の従業員を監視するという発想がシンフォーム側に欠落していたと認められる[24]。

---

(20) ベネッセコーポの基盤本部IT戦略部長（当時）であった樋口康弘氏は，「ベネッセでは，ITの重要性にかんがみ，早くから戦略性を重視した組織づくりを進めてきました。本社の「IT戦略部」は，事業部門案件のコントロールと全社共通基盤のシステム企画・要件定義・開発標準化およびガバナンスを，そしてシステム子会社である「株式会社シンフォーム」はそれらの案件の設計から構築とシステム運用・保守を担うという役割分担のもとに業務を推進しています」（行政＆情報システム2010年8月号「激動の時代だから「可視化」と「標準化」を根底に置いて」2頁）と語っている。

(21) 「事業会社のベネッセとシンフォーム，親会社のベネッセホールディングスの役割分担が明確でなく，相互にチェックが効きにくい体制だった」（日経コンピュータ2014年10月2日号「4800万人の情報漏洩でベネッセが決断」7頁）。

(22) 事件後の対策として，ベネッセでは，データベースの管理をベネッセHDの業務とし，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級執行役員のCLO（Chief Legal Officer）と，同人の下で情報セキュリティの監査を担当するCISO（Chief Information Security Officer）を任命するとともに，その担当部署としてDB管理本部を設置した。また，データの保守・運用の実務については，グループ外の情報セキュリティ専門企業との間で合弁企業「ベネッセインフォシェル」（ベネッセHDの出資比率70%）を新たに設立し，シンフォームから所要の資産や人員を同社に移管した。

(23) 「幼児を含む個人情報を全人口の3分の1以上もの規模で蓄積してきたベネッセを，ほかの一般企業と同列視することはできない」（日経ビジネス2014年9月29日号「ベネッセ，覆水の始末　③陥穽」26頁）。
「「ベネッセの最も重要な資産は会員名簿」今年6月に最高顧問に退いた創業家の福武總一郎はかつて，周囲に何度もそう語っている」（日経ビジネス2014年9月22日号「ベネッセ，覆水の始末　②慢心」26頁）。

(24) 「シンフォームは，A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。（中略）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」（調査委員会（2014），7頁）。

一般的に，業務委託先の従業員については，社員よりも忠誠心が低く，内部不正のリスクが高いと考えられるが，身元の確認などの初歩的対応さえ実施していなかった[25]。シンフォームでは，システムの保守・管理業務を広範に外部委託していたことにより，事業者としての責任感を喪失していたと推察される[26]。

ちなみに，シンフォームの社内規程では，認証IDとパスワードを設定してアクセス管理を行い，さらにパスワードを定期的に更新することとしていた。しかし実際の運用では，定期的なパスワードの更新は行われておらず[27]，さらに認証IDやパスワードも共同で利用する状態であったとされる[28]。Aが正規のアクセス権限を有していた以上，このようにアクセス管理が杜撰であった事実は本事件の原因とは言えないが，シンフォームが責任感を喪失していたことの傍証と認められる。

その他の3件の問題点については，5.で後述する。

5. 情報活用優先の経営方針

ベネッセグループでは，前述のとおり顧客情報を大量に収集していたが，その収集経路が多種多様で同一人物の情報が重複して登録されていた上に，その分析にも多大の時間を要するという問題が生じていた。その一方で，子供の学年別にダイレクトメール（DM）を発送するという従前のマーケティング手法は，消費者の多様化及び塾との競争激化により陳腐化しつつあり，新たなマーケティング手法を開発する必要に迫られていた[29]。

「DB管理の業務は，3重の委託契約を経て，容疑者に委ねられていた。事業会社のベネッセコーポレーションからグループ企業のシンフォームに，シンフォームから外部企業に，外部企業から容疑者に，である。（中略）コスト削減のため顧客DB管理を外部企業に丸投げしたまま，適切な監視や権限管理も行わず，実際にデータに触れるSEの給与や待遇も知らないようでは，個人情報を預かる「データオーナー」としての責任を放棄したのと同じだ」（日経コンピュータ2014年8月7日号「ベネッセホールディングス　空前「2300万件漏洩」の真因」58頁）。

(25) 調査委員会（2014）は，個人情報を取り扱う業務を委託する場合には，業務担当者について履歴書の確認や面談などの事前審査を行うとともに，社員による行動監視体制を構築すべきと提言している（同11頁）。また，事件後の対策として，ベネッセでは，業務委託先の担当者には，個人情報へのアクセス権を付与しないこととした。

(26) ベネッセコーポの基盤本部IT戦略部長（当時）であった樋口康弘氏は，「シンフォームは，増える一方の開発案件の多くを自社の要員で対応できず他社にアウトソーシングした結果，内部のITスキルが低下するという二重の空洞化が進んだことです。アウトソーシングというと聞こえは良いのですが，業者に丸投げになっていたのです」（行政＆情報システム2010年8月号「激動の時代だから「可視化」と「標準化」を根底に置いて」2頁）と語っている。

(27) 「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」（調査委員会（2014），10頁。傍点筆者）。

(28) 「弁護側は冒頭陳述で，顧客データについて「アクセスするIDとパスワードは共同利用で，別のサーバー内のファイルに記載されており，（付与された従業員以外も）容易に参照できた」と主張」（毎日新聞2014年11月14日地方版）。
「（弁護側は，）情報にアクセスするためのID，パスワードが個人に付与されるのではなく共同利用だった（と指摘した）」（東京新聞2014年11月14日地方版）。

(29) 「顧客情報を基に，国内最大規模に上る件数のダイレクトメール（DM）を配布して顧客を獲得するのが，進研ゼミのビジネスモデル。だがDMの効果が落ちている上，共働き夫婦の増加で親が面倒を見る必要のある通信教育は，学習塾に顧客を奪われている」（日経ビジネス2014年4月7日号「ベネッセ，蘇生かけ原田氏登用」15頁）。

こうした背景を踏まえて，ベネッセグループでは，2010年に顧客情報を一元管理する「新顧客基盤」と呼ばれるシステムの運用を開始した。それによって，これまでの学年別の区分よりもはるかに細かく，個々の顧客のニーズに応じて「個別シナリオ化」したマーケティング活動が可能となった[30]。

ベネッセグループが，このように顧客情報を積極的に活用する経営方針を採用したこと自体は戦略的に妥当であろう。その一方で，情報活用の優先に伴って，それとトレードオフの関係[31]にある情報セキュリティが相対的に軽視されたことが事件の一因と認められる。

4.3で前述したように，シンフォームでは，アクセス範囲を未区分にして，担当者が顧客情報全体にアクセスできるようにしていた。これは，「個別シナリオ化」の新しいマーケティング手法を開発していくためには，様々な経路で収集した顧客情報に対して確実な「名寄せ」（個人特定）を実施するとともに，PDCAサイクルに基づき広範なデータの組み合わせを試行錯誤する必要性があったためと推察される。

4.5の「アラートシステムの未設定」については，アラートシステムの趣旨から考えて，クライアントPCをアラート対象としていなかったのは不可解である。シンフォームでは，前述のマーケティング手法開発の関係で，データベースに頻繁にアクセスして大量の情報処理を行っていた。そのため，アラートシステムが機能していると，頻繁にアラートが発せられてしまって管理者の負担となることから，敢えて未設定にしていたのではないかと推察される[32]。

4.6については，前述のとおりベネッセグループでは，情報活用に関する体制を構築する一方で，情報セキュリティについては責任者や担当部署を決めていなかった。これも，情報活用と比べて情報セキュリティを軽視していたため，その体制を構築する必要性を認識していなかったと考えられる。

このように情報活用に偏重した状況が放置されていたのは，ベネッセグループの経営者にITリテラシーが不足しており，十分な情報セキュリティ対策が取られているはずとの過信が存在したためである[33]。

---

(30) ベネッセコーポのIT戦略部成績・マーケティング基盤担当部長（当時）であった保本尚宏氏は，「私たちは，ダイレクト・マーケティングの方向性として，『個別シナリオ化』という深化の方向性を定めました。これは，年齢（学年）別という従来のセグメンテーションに加えて，お子様の学校別や地域別，学習スタイル，あるいは行動別といった細かなセグメンテーションを用いて，お客様へのアプローチをよりパーソナライズしていくということです」（Oracle Data Intelligence Forum 2013 レポート「ベネッセは，オラクルのBIテクノロジーを活用してダイレクト・マーケティングのさらなる深化／進化を目指す」）と語っている。

(31) この情報活用と情報セキュリティのトレードオフ関係について，海上自衛隊のイージス防衛秘密流出事件を分析した樋口（2010）は，「情報管理については，「迅速かつ柔軟な情報利用」と「着実かつ形式主義的な情報保全」という矛盾する命題が同居している。前者の情報利用を優先するのであれば，情報保全の手続きは簡素とならざるを得ず，それだけ情報流出のリスクは高くなる。また，後者の情報保全を重視すれば，必然的に手続きは煩雑となって，前者の情報利用が阻害される」（同79頁）と指摘した。

(32) ちなみに，本事件を受けての改善策として，調査委員会（2014）は，「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」（同12頁）と述べている。アラートシステムが機能していたケースでも，閾値が緩いレベルに設定され，それだけアラートが発せられにくい状況であったと考えられる。

(33)「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」（調査委員会（2014），7頁）。
「弊社としての根本的な問題点は，自社の情報セキュリティに関する過信，経営層を含むITリテラシーの不足，性善説にたった監査，監視体制の運用，などの企業風土に起因する甘さにあると判断しました」（ベネッ

本来であれば，グループ内でシステム管理を担当していたシンフォームが，経営者に対して積極的に助言するとともに，自らも問題点の解消に努めるべきであった[34]。しかし，グループ内の支援部門という位置づけのシンフォームは，やむを得ないことではあるが，事業部門に対して受動的になりがちであり，情報セキュリティ面での問題提起に消極的になってしまったと考えられる[35]。

6. 事件の原因メカニズム

本事件の原因メカニズムを三分類・因果表示法にしたがって整理[36]すると，以下のとおりとなる（図1参照）。

①直接原因

原因A　内部不正によって大量の顧客情報を漏えいしたこと

②Ⅰ種潜在的原因

原因B　書出し制御システムの不備

原因C　私物機器持ち込みの放任

原因D　アクセス範囲の未区分

原因E　アクセスログの未確認

原因F　アラートシステムの未設定

原因G　不明確なセキュリティ責任者及び担当部署

③Ⅱ種潜在的原因

原因H　IT業務の特殊性（I，Kの背景）

原因I　シンフォームの知識不足（B，Jの背景）

原因J　シンフォームの責任感の不足（C，Eの背景）

原因K　経営者の認識不足（Lの背景）

原因L　情報活用優先の経営方針（D，F，Gの背景）

セHDニュースリリース（2014年9月10日付））。

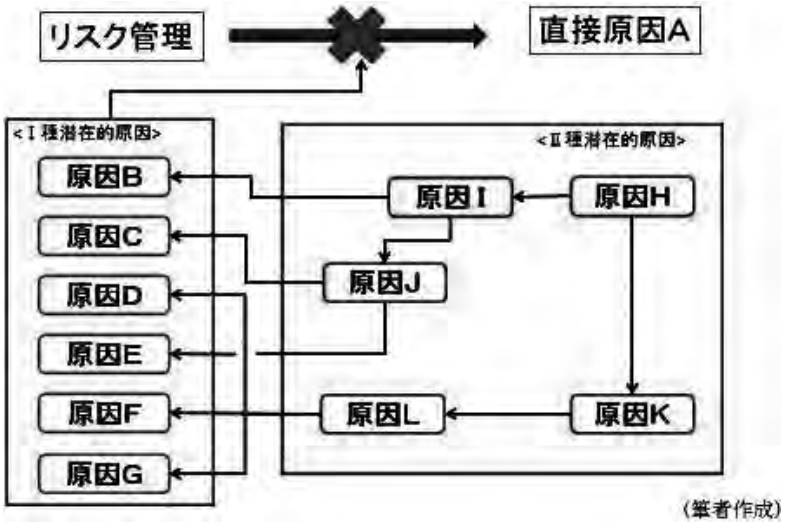
(34) 2011年6月から2013年3月にかけて，ベネッセコーポの代表取締役副社長がシンフォームの代表取締役社長を兼務する人事措置が行われた（その後，同人はベネッセコーポの代表取締役社長に昇格）。すなわち，この時点でのグループ内におけるシンフォームの位置付けは決して低いものではなく，情報セキュリティに関してイニシアティブを発揮しうる立場にあったと認められる。

(35)「シンフォームについてみると，その重要な顧客であるBC（筆者注：ベネッセコーポのこと）の事業部門の意向に従わざるを得ない傾向が認められ，（中略）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」（調査委員会（2014），6-7頁）。

(36) 三分類・因果表示法は，組織不祥事の原因メカニズムを包括的に理解するために，筆者が樋口（2011）で考案したフレームワークである。組織不祥事の原因を直接原因とⅠ種・Ⅱ種潜在的原因に分類した上で，因果関係の連鎖の中で一段階上流側に位置することを「背景」と付記し，原因メカニズムの図示に当たっては，矢印の方向で背景を表示する。

直接原因とは，組織不祥事を発現させる直接の引き金となった問題行動であり，何らかの違反行為が組織不祥事を構成するケースでは，当該違反行為自体が直接原因となる。潜在的原因とは，直接原因を誘発又は助長した因果関係に連なる組織上の問題点であり，直接原因の発生を防止するためのリスク管理の不備に関するⅠ種潜在的原因と，それ以外のⅡ種潜在的原因に大別される。詳しくは樋口（2011）を参照されたい。

図1　事件の原因メカニズム



（筆者作成）

7. 考察

本事件を誘発した原因メカニズムとして，業務委託先に対する管理を懈怠し，基本的なセキュリティ対策さえ実施していなかった問題に関して「委託側の責任感喪失のリスク」，IT 業務に関する経営者の理解が不足し，セキュリティ対策が軽視された問題に関して「傍流事業の特殊性による組織不祥事リスク」の2類型が認められる。

7.1 委託側の責任感喪失のリスク

樋口（2012a）は，2004年発生の関西電力美浜原発配管破損事故，2006年発生のふじみ野市プール事故及び2007年発覚の関西テレビ「発掘！あるある大事典Ⅱ」捏造事件を分析し，アウトソーシングによって組織不祥事が誘発されるメカニズムの一つとして，「委託側の責任感喪失のリスク」を指摘し，「ノウハウの喪失又は長期継続的関係が原因で委託企業が責任感を喪失し，受託企業に対する監督が不在となるリスク」（同143頁）と定義した。

その後も，2011年発生の東海テレビ「ぴーかんテレビ」不適切テロップ事件を分析した樋口（2013a）及び同年発生の東京ドーム遊戯施設「舞姫」における死亡事故を分析した樋口（2014）は，これらの事件の潜在的原因として，現場における作業内容の教育を企業側が自ら実施すべきであったにもかかわらず，外部スタッフやアルバイトに任せきりにしていたと指摘し，同様に「委託側の責任感喪失のリスク」を抽出した。

本事件のセキュリティ対策上の問題点のうち4.2の「私物機器持ち込みの放任」及び4.4の「アクセスログの未確認」に関しては，4.7で前述したように，システムの保守・管理業務を広範に外部委託していたことでシンフォームが事業者としての責任感を喪失し，業務委託先の従業員に対する監視を怠っていたことが原因であり，「委託側の責任感喪失のリスク」が発現したものと認められる。

経営実践上の含意としては，システム関係の業務では，コスト削減の観点から広範に

アウトソーシングを行うことが通例であるが，業務の一部を敢えて外部化せずに社内（グループ内）に残すことで，業務委託先を監督するノウハウや事業者としての責任感を保持する方策が挙げられる[37]。また，業務委託先に対する監視が困難な場合には，アウトソーシングを止めるという選択肢も検討する必要があろう[38]。

ちなみに，情報処理推進機構（2013）は，本事件を受けて，2014年9月に内容を一部改定した際に，業務委託時の対策のポイントなどに関する記述を詳細化するとともに，「委託期間中，委託先や，その他第三者が提供するサービスにおいて，自組織の基本方針に照らし，適切な内部不正防止対策が確認できない場合には，契約先を切り替える，または組織外への委託を中止することも検討します」（対策4（16），傍点筆者）と追加した。

7.2 傍流事業の特殊性による組織不祥事リスク

樋口（2012b）は，2010年に発覚したメルシャンの水産飼料事業部における循環取引事件について分析し，事件の潜在的原因として，問題の水産飼料事業部が社内で傍流事業の位置付けで事業内容も特殊であったため，経営者の関心や知識が不足するとともに，事業部内の人事が閉鎖的で長期配置が通例となっていたことを指摘した。その上で，こうした組織不祥事を誘発するメカニズムを「傍流事業の特殊性による組織不祥事リスク」と整理し，「傍流事業の特殊性のために監督が不十分になるとともに，人事配置も閉鎖的・長期的になるために，組織不祥事が誘発されるリスク」（同81頁）と定義した。

また，2011年に発覚した東海ゴム工業の労働安全衛生法違反事件について分析した樋口（2013b）も，事件の潜在的原因として，ボイラー保守業務の特殊性により，補修担当者の人事が長期配置となって異議の提出が心理的に困難になるとともに，上級管理者の監督が疎かになっていたと指摘し，同様に「傍流事業の特殊性による組織不祥事リスク」を抽出した。

本事件に関しては，5.で前述したように，ベネッセグループの経営者は，専門的な分野であるIT業務について十分なリテラシーを持ち合わせておらず，情報セキュリティに関する認識が乏しかったために監督が疎かになったものである。ただし，「傍流事業の特殊性による組織不祥事リスク」の定義中の「人事配置も閉鎖的・長期的になる」という部分については，シンフォームの業務の専門性や独立した人事採用の状況などから推測できるが，事実関係は必ずしも明確でない。そのため，本事件に関しては，「傍流事業の特殊性による組織不祥事リスク」が発現した可能性が高いと指摘するにとどめる[39]。

経営実践上の含意としては，IT関係の専門知識をあらためて経営者に修得させることは

---

(37) 事件後の対策として，ベネッセHDでは，システムの保守・管理業務を担当する新会社を情報セキュリティ専門企業と合弁で設立し，グループ外への業務委託を禁止することにした。また，システムの開発業務に関しては，グループ外への業務委託を許容するが，再委託を原則として禁止した上で，例外的に再委託を認める場合には，再委託先の信用性を確保するために，ベネッセが作成するガイドラインを遵守させることとした。

(38) 現状では，企業側がアウトソーシングのリスクを認識せず，十分な監視措置を講じていない（＝監視対策に必要なコストを負担していない）ために，アウトソーシングのコストを安価と誤認しているケースが少なくないと考えられる。

(39) 「傍流事業の特殊性による組織不祥事リスク」の定義中の「人事配置も閉鎖的・長期的になる」については，上級者による監督が不十分となる態様の一つにすぎず，必須の要件と考えるべきではないとの整理もあり得る。今後の研究では，「傍流事業の特殊性による組織不祥事リスク」の定義規定の見直しも検討課題の一つとしたい。

難事であり，また，そのような専門的人材の中に経営者としての適任者を見つけることも容易ではない。したがって，外部の専門企業あるいは有識者に依頼して，IT業務に対する外部監査の実施，あるいは専門的な助言や提言を求めることが適当である(40)。

おわりに

本事件の調査報告書である調査委員会（2014）は，事実関係の説明が非常に不足しており，内容を理解することが難しい箇所が少なくない。その背景として，調査委員会の位置付けが，「企業危機に対応するための，B会長兼社長の諮問機関としての調査委員会であり，（中略）いわゆる日弁連ガイドライン型第三者委員会ではない」（調査委員会（2014），2頁）とされ，部外に対する説明を主眼としていないことが挙げられる。

そのため筆者は，ベネッセHDに対して本研究への協力を求め，その了解を得た後に，調査委員会（2014）の内容を確認するための質問事項を送付した。しかし，それに対するベネッセHDの回答は著しく遅延した上に，質問項目のほとんどについて回答を差し控えるとのことであり，実質的に意味のある情報はほとんど得られなかった。

その後も，筆者は繰り返し説明を求めたが，何の進展もなくいたずらに時間が経過するだけであり，ついにベネッセHD側からの情報収集を断念するに至った。本稿において，事実認定の資料として新聞や雑誌の記事を多用せざるを得なかったのはそのためである。調査報告書の内容確認という最低限の情報さえ提供されなかったケースは，筆者のこれまでの組織不祥事研究でも非常にめずらしい。

こうした対応ぶりの背景には，ベネッセHD側が「ご指摘いただいているセキュリティ対策上の問題点につきましては，（中略）今後の民事訴訟においても，同様の点が争点となることも予想されるので，敢えてコメントは控えさせていただいております」（2015年3月11日付けのベネッセHDからの返信メール）と述べているとおり，情報漏えいの被害者からの民事訴訟に備えて，なるべく情報を部外に出したくないという発想が存在するように思われる。

しかし，それでは何のために不祥事の調査報告書を公表するのだろうか。企業の社会的責任の一環として，外部のステイクホルダーに対する説明責任を果たすためではないのだろうか。そして，ベネッセHDにとって最も重要なステイクホルダーの中に，情報漏えいの被害を受けた顧客の皆さんが入っていることは言うまでもない。

不祥事の事実関係をありのままに説明し，その結果として損害賠償を支払うことになったとしても，それは顧客に対して企業が果たすべき当然の責任であろう。調査報告書の発表が，説明責任を果たすという本来の趣旨から外れて，不祥事の幕引きのための「禊（みそぎ）」のように扱われることは，決してあってはならない。

---

(40) 事件後の対策として，ベネッセHDでは，前述のCLOについて，グローバル企業での専門性の高い実績を持つ人材を招聘するとともに，情報セキュリティや個人情報に関する有識者により構成される外部監視機関を設置し，①情報セキュリティ全般について助言・提言すること，②再発防止策の実施・運用状況を確認すること，③情報セキュリティシステムが安全に機能しているか確認すること等の業務を実施させることとした。

＜参考文献＞

JNSA・情報セキュリティ大学院大学（2015）『2013年　情報セキュリティインシデントに関する調査報告書　―個人情報漏えい編―　第1.1版』
経済産業省（2012）『「営業秘密の管理実態に関するアンケート」調査結果』
社会安全研究財団（2010）『情報セキュリティにおける人的脅威対策に関する調査研究報告書』
情報処理推進機構（2012）『組織内部者の不正行為によるインシデント調査　―調査報告書―』
情報処理推進機構（2013）『組織における内部不正防止ガイドライン』
調査委員会（2014）『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』
樋口晴彦（2010）「イージス防衛秘密流出事件」『捜査研究』59（6），76-82頁
樋口晴彦（2011）「組織不祥事の原因メカニズムの分析　―18事例に関する三分類・因果表示法を用いた分析と原因の類型化―」『CUC Policy Studies Review』30号，13-24頁
樋口晴彦（2012a）『組織不祥事研究　―組織不祥事を引き起こす潜在的原因の解明―』白桃書房
樋口晴彦（2012b）「メルシャン循環取引事件の事例研究」『千葉商大論叢』50（1），71-83頁
樋口晴彦（2013a）「東海テレビ「ぴーかんテレビ」不適切テロップ事件の事例分析」『千葉商大論叢』50（2），223-236頁
樋口晴彦（2013b）「東海ゴム工業の労働安全衛生法違反事件の事例研究」『危機管理システム研究学会研究年報』第11号，1-9頁
樋口晴彦（2014）「東京ドーム遊戯施設「舞姫」における死亡事故の事例研究」『日本経営倫理学会誌』第21号，221-233頁

（2015.6.22受稿，2015.7.17受理）

— Abstract —

Study of the Leakage Case of Customer Information in Benesse Holdings

As the causes to induce the internal crime, the study pointed out six failures of the system security: delay of updating the export control system, neglect of checking the carry-over of personal devices, no division of the access range, neglect of checking access log, unset alert system, and no designation of chief security officer. One of the backgrounds of the case is the management strategy to prioritize the active use of information.

The study extracted two typical mechanisms to induce organizational misconducts from the case. The first risk is the loss of the sense of responsibility, which led to the neglect to monitor outsourcing. The second risk is the particularities of business, which led to the board's little understanding of IT business.