法とシステム監査研究プロジェクト 成果報告

システム監査学会第３４回研究大会

開催日：２０２０年１１月６日（金）
発表：荒木哲郎（弁護士・システム監査技術者）

序　概要

1　研究プロジェクトの概要

■　主査　弁護士　稲垣隆一

■　概要

国、自治体、企業の遵法経営のために情報システムの企画、開発、運用、保守が抱える課題と、課題解決のためのシステム監査の経営における位置づけ、監査の尺度、監査技法を研究して、コンプライアンス経営のためにシステム監査が果たし得る実務的な役割を明らかにする。

「法とシステム監査研究プロジェクト」メンバー
（原則　五十音順）

氏名	所属等	備考
稲垣　隆一	稲垣隆一法律事務所・弁護士	主査
黒澤　兵夫	TAKE国際技術士研究所	副主査
多和田　肇	システム監査技術者CIA,CISA	
成田　和弘	システム監査技術者CIA,CISA	
牧野　博文	東芝	
芳仲　　宏	東京地方裁判所	
荒木　哲郎	弁護士・システム監査技術者	発表

2　研究テーマ

大規模情報漏えい事件に関する裁判例から考えるシステム監査のポイント

３　今回のテーマを選択した趣旨

- 大規模に個人情報が流出した事件である、いわゆるベネッセ顧客情報漏えい事件については、２０１９年に２つの高裁判決が出され（東京高裁令和元年６月２７日判決【判決１】、（大阪高裁令和元年１１月２０日【判決２】。）、どちらも、直接に個人情報を管理していた開発の業務受託会社のみならず、業務委託会社にも逆転で損害賠償責任を認めている。

- 本報告では、２つの裁判例を比較すると共に、システム監査において注意すべき点等について、システム管理基準との関係から検討した内容等を報告する。

４　発表内容

第１　事案の内容

第２　判決の検討

第３　システム監査におけるポイント

本論
第１　事案の内容

１　概要

通信教育事業等を営むベネッセ社。（以下「B社」という。）から委託を受けてB社が取得した個人情報を分析するシステムの開発、運用等をしていたシンフォーム社（「以下「S社」という。）の業務委託先の従業員（以下「W」という。）において、顧客の個人情報が外部に漏えいしたことにより精神的苦痛を被ったとして、控訴人（原告）が、不法行為に基づき、慰謝料及び遅延損害金の支払を求めた事案

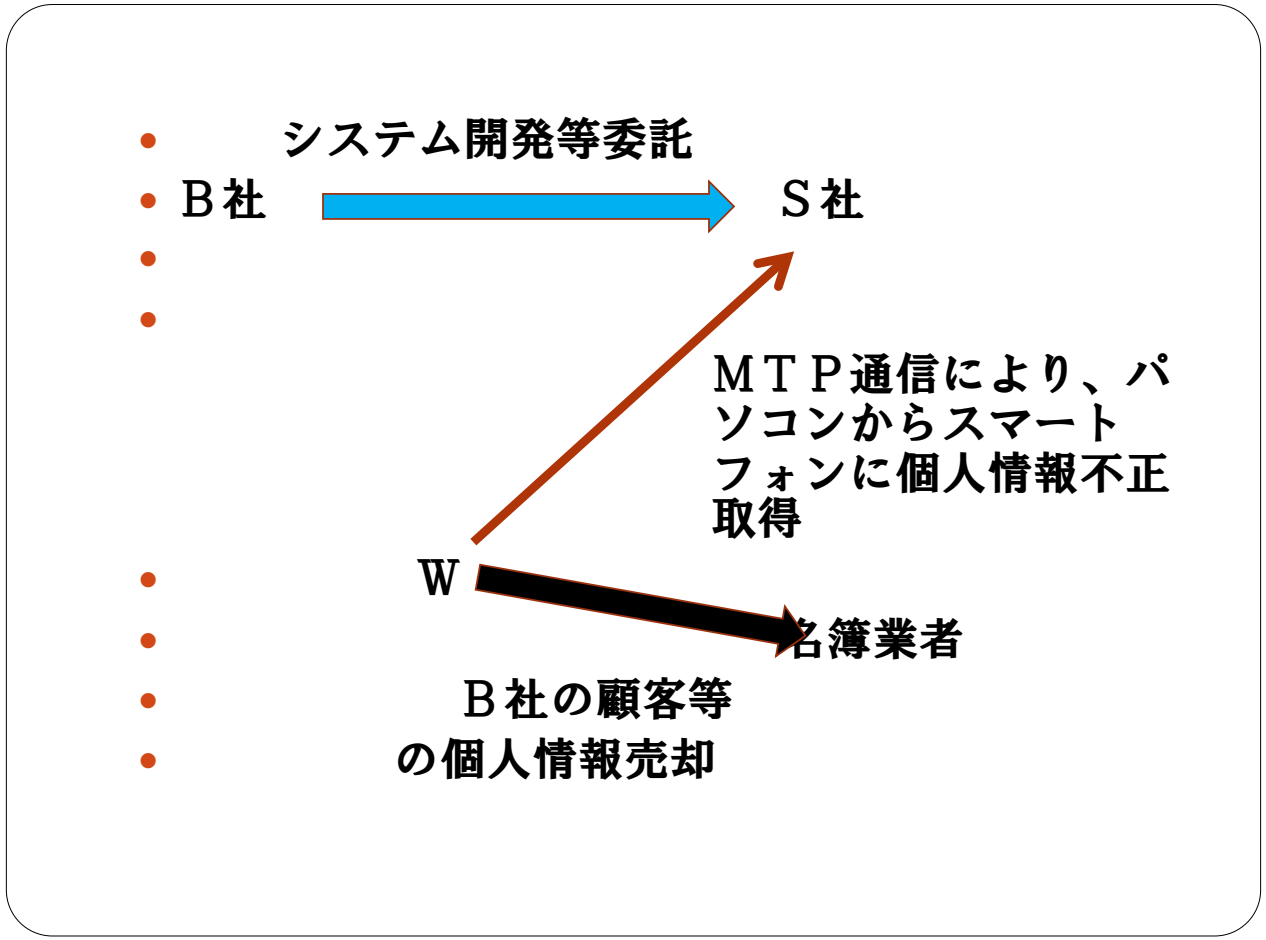
2　事実経過

H24.4　Ｂ社がＳ社にシステムの開発・運用・保守の業務を委託（Ｓ社は複数の業者に再委託）

- 再委託先の従業員であったＷは、本件データベースにアクセスするためのアカウントの提供を受け、Ｓ社から貸与を受けた業務用のパソコンを使用し、業務に従事していた。

H25.7～26.6

Ｗがパソコンからｍｔｐ（メディア・トランスファー・プロトコル）に対応したＷ所有のスマートフォンに個人情報（４８５８万人分）を転送する方法により不正取得し、その後名簿業者に売却



H27.12.2　判決２の地裁判決

- 原告（控訴人）の氏名が漏えいしたことのみを認定した上で、これが被控訴人の過失によるものであることを基礎付けるに足りる具体的事情の主張立証がないとして、請求を棄却。

H28.6.29　判決２の（差戻前）高裁判決

- 控訴人の個人情報の漏えいについて、不快感等を抱いただけでは，これを被侵害利益として，直ちに損害賠償を求めることはできないものと解されるとして、控訴を棄却。

H29.10.23　判決２の最高裁判決

- 本件漏えいによって控訴人はそのプライバシーを侵害されたといえるところ，原審はその点について審理を尽くさなかった違法があるとして，原判決を破棄し，被控訴人の過失の有無並びに控訴人の精神的損害の有無及びその程度等について更に審理させるために本件を差し戻した。

H30.6.20　判決１の地裁判決

　Ｂ社の予見可能性は否定したものの、Ｓ社の注意義務違反は認めたが、Ｗに対する使用者責任は否定し、結論としては、被告側の対応（金券の配布）等から、原告らに損害なしとして、請求棄却。

- R1.6.27　判決１
- 　Ｓ社及びＢ社の過失を認め、両社に被控訴人らに対し、２０００円ずつの損害賠償義務を認める。

- R1.11.20　判決２（差戻判決）
- 　Ｂ社（及びＳ社）の過失を認め、Ｂ社に被控訴人に対し、１０００円の損害賠償義務を認める。

3　本件の裁判上の争点

- （1）S社の予見可能性の有無
- 　本件で、Wは、MTP（に対応したW所有のスマートフォンを業務用パソコンのUSBポートに接続する方法で、個人情報を取得したが、本件当時、S社は、業務用パソコンにおいて、MSC（Mass Storage Class）によるデータ通信に対しては、書き出しを制御する措置を施していた。
- 　当時、MTPは、まだ普及率が高くなく、注意義務の前提として、本件当時、MTP通信でデータを転送する方法によって個人情報を不正に取得されることを予見し得たかが問題となった。

（２）Ｓ社の注意義務違反の有無

（１）で予見可能性ありとした場合、適切な措置を取るべき注意義務を怠ったか否か。

（３）Ｂ社の予見可能性の有無

（４）Ｂ社の委託先（Ｓ社）選任及び監督にかかる注意義務違反の有無

（（５）使用者責任の成否）

直接の責任が否定された場合問題。

（６）　損害賠償額

４　判決１の内容
（１）Ｓ社の予見可能性について

「スマートフォンを、ＵＳＢケーブルでパソコンと接続してデータのやり取りをすることが可能であることは、一般的に知られており、ＭＴＰも、データの転送に用いる規格として新規で特殊なものとはいえない。」（中略）

「デバイスやＯＳは、バージョンアップにより高機能化していくものであるから、それに応じて、接続されるデバイスを制御してデータの漏えいを防いでいく必要がある。被控訴人らは、本件セキュリティソフトを導入していたことからして、このような必要性を具体的に認識していたものと認められ、また、本件漏えいは、一般的にいっても、特殊な知識や技術を用いた予見が困難な態様のものではなく、むしろ、デバイスやＯＳの高機能化によって発生する危険の範囲内のものというべきであるから、予見可能性は否定されない。」

（２）Ｓ社の注意義務違反について

- 「本件業務において、業務用パソコンについてＭＴＰを使用してデータの転送を行う必要性はなかったと認められる。
- そうすると、本件において、ＭＴＰを使用するデバイスの使用が許可されていたのは、単に被控訴人シンフォームにおいて、本件セキュリティソフトの設定の確認を失念ないし怠っていたことによるものというべきである。そして、被控訴人Ｓ社は、本件漏えいまでにＭＴＰ対応スマートフォンに対する書き出し制御措置を講ずることが可能であったから、そのような措置を講ずべき注意義務があったにもかかわらず、これを怠った点に過失があったと認めるのが相当である。」

（３）Ｂ社の注意義務違反について

- 「他方、被控訴人Ｂ社において、被控訴人Ｓ社に対し、ＭＴＰ対応スマートフォンに対する書き出し制御措置が講じられているか否かを確認すべく、本件セキュリティソフトの設定状況について適切に報告を求めていれば、ＭＴＰ対応スマートフォンに対する書き出し制御が十分でないことを知り、本件セキュリティソフトの使用可否制御を指示することができた（中略）。そうすると、被控訴人Ｂ社は、被控訴人Ｓ社が、本件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を負っていると解されるところ、被控訴人Ｂ社において本件セキュリティソフトについて適切な設定が行われていると誤信していたことにより、適切な監督を行うことができなかったものであるから、上記注意義務に違反した過失があると認めるのが相当である」

５　判決2の内容
（１）予見可能性について

- 「Ｓ社において、上記のように個人所有のスマートフォンを業務用ＰＣに接続することを容認する以上は、本件漏えい当時，業務委託先の従業員が持ち込む可能性のあるすべての私物スマートフォンについて、それが業務用ＰＣのＵＳＢポートに接続されることで個人情報を不正に取得されるリスクがあるか否かを日常的に調査確認し、そのリスクがあれば、これを防止する措置を講ずべき必要性を認識していたものと認められる。そして、本件漏えい当時においても、Ｓ社が、以上の点について必要な調査確認を行っていれば（本件セキュリティソフトの製作業者に確認するなど）、ＭＴＰ対応のスマートフォンが流通していたことを容易に把握することができたと認められ，このようなスマートフォンが業務用ＰＣのＵＳＢポートに接続されることによって個人情報を不正に取得されるリスクがあることや、本件セキュリティソフトによって、そのリスクを回避できるか否かを容易に認識しえたと認められる。」

（２）Ｓ社の注意義務違反について

- **Ｓ社は，本件漏えい当時、被控訴人から業務上の必要によって利用することを許されていた本件個人情報を含む大量の個人情報について、業務委託先の従業員に業務用ＰＣを利用してアクセスすることを認めていたところ、これらの従業員が業務用ＰＣに個人所有のスマートフォンを接続することを容認していたというのであるから、業務委託先の従業員がＭＴＰ対応スマートフォンを執務室内に持ち込んで、上記個人情報に接することのないように適切な措置を採るべき注意義務を負っていたというべきであり、これを怠ったことについて過失があるというべきである。（中略）**

- 「控訴人の注意義務違反の主張は選択的であるから、本件においては、その余の義務違反については検討するまでもないところであるが、Ｓ社において、他の結果回避措置を採ることで義務違反を免れることもできる関係にあるから、書出し制御措置を講じる義務を負っていたかについても検討する。」
- 「仮に，執務室内への私物スマートフォンの持込み禁止措置を行わないのであれば、情報漏えいを防ぐのに実効性が高く、かつ業務従事者に対して必要以上に制約が生じない方法でもあった情報の書出し制御措置ないしＷＰＤデバイス使用制御措置を採るべき義務があったと解される。」
- 「本件セキュリティソフトにより、特定のＵＳＢメモリ以外は全てが使用できなくなっていると思っていたために、上記対策をとることを怠っていたことが認められる。」

（３）Ｂ社の注意義務違反について

- 被控訴人（Ｂ社）は、本件漏えい当時、本件漏えいの方法による個人情報の漏えいの危険性を予見し得たにもかかわらず、株式会社Ａに対し、本件セキュリティソフトがＭＴＰ対応スマートフォンに対する書出し制御機能等を備えているか否か、株式会社Ａの業務委託先の従業員が、被控訴人が管理する個人情報にアクセスすることができる業務用ＰＣのＵＳＢポートに個人の所有するスマートフォンを接続できる状況にあったかどうかについて適切に報告を求めていなかったもので、これらについて適切に指導監督を行っていれば、ＭＴＰ対応スマートフォンに対する書出し制御機能に対応したセキュリティソフトへの変更を指示するか、あるいは、本件セキュリティソフトのままであっても、ＭＴＰ対応スマートフォン（ＷＰＤデバイス）に対する使用制御措置を採るように指示することができたものであり、それが困難であったとしても、株式会社Ａに対し，業務委託先の従業員が本件個人情報を含む大量の個人情報に接することができる執務室内に、個人のスマートフォンを持ち込むことを禁止するよう指示することができた」

- →注意義務違反あり。

6　両判決の比較

	当事者（被控訴人）	予見可能性	S社の注意義務またはB社の監督義務の対象
東京高裁(判決１)	B社及びS社	MTP対応スマートフォンの普及の程度にかかわらず、デバイスの接続によるデータの漏えいの防止の必要性を認識していれば足りる。	MTP対応スマートフォンに対する書き出し制御措置
大阪高裁(判決②)	B社	調査等をしていれば、MTP対応のスマートフォンの流通していたことを容易に把握することができた。	①私物スマートフォンの持込み禁止措置 ②書き出し制御措置 ③WPDデバイス使用制御措置 （①乃至③は、選択的）

第２　判決の検討

１　注意義務及び監督義務の対象

判決２（大阪高裁）の方は、複数の措置について検討している。

↓

３つの措置は選択的→どれか１つを採っていれば情報漏えいは起きなかった。（本件では、どれも採られていなかった。）

↓

判決２の方が妥当と考えられる。

（判決１は弁論主義【事実・証拠の収集を当事者の権能と責任に委ねるという原則】から、他の手段が検討されなかった？）

２　Ｂ社の監督義務違反

どちらの判決でも、（あっさりと）認められている。

→最高裁が、Ｂ社の責任を認める方向にした以上、今後も肯定する方向の判決が続くと思われる。

参考

①東京地裁平成３０年１２月２７日判決

予見可能性否定（使用者責任でＳ社に対する損害賠償を認める。

②東京地裁平成３０年６月２０日判決

請求棄却（同日の判決１の地裁判決と同様）

③東京高裁令和２年３月２５日判決（①の控訴審）

Ｂ社の責任（監督の注意義務違反）を認める判決（慰謝料１人当り３３００円）。

参考　③東京高裁令和２年３月２５日判決（①の控訴審）

（１）予見可能性については、肯定

（２）注意義務について、大阪高裁と同様に複数の措置について検討している。

ただし、

①スマートフォンの持ち込み禁止措置

&

②USB接続禁止措置

→過度な制約として、禁止措置を講ずべき注意義務を否定

③情報の書き出し制御措置

→実効性があり、業務従事者に対して必要以上に制約が生じない方法として、注意義務あり。

④アラートシステムの設定義務違反

（一定量の情報が一度移動した際に警告がでるシステムの対象外とされていた。）

→誤動作の防止のため必要があり、また、一定量の基準を高くせざるを得ず、本件漏えいを回避できたとは認められないとして、否定。

⑤監視カメラ等による監視義務違反

→現に設置されていたものより高精度な監視カメラを設置していたとしても、本件漏えいを回避できたとは認められないとして否定。

③の点から、S社の過失責任、及び、B社の監督に関する注意義務違反認める。

第３　システム監査におけるポイント

- １　Ｓ社の問題点(判決で取り上げられていない点も含む。《★は取り上げられている点》）
- （１）設定に関する知識不足。設定不十分《★》
- （２）私物機器持ち込みの放任《★》
- 　　（カメラで取れば持ち出せるのでは。）
- （３）アクセス範囲の未区分
- 　　ただし、本件では、wに本来の権限あり。

- （4）アクセスログの未確認
- 　　アクセスログの記録はあり。
- （5）アラートシステムの未設定
- 　　頻繁に鳴ることの防止のため
- （6）セキュリティ責任者・担当部署が不明確
- 　　Ｓ社の権限不明確

- 【参考】
- 樋口晴彦氏「ベネッセ顧客情報漏えい事件の事例研究」

2　対策（監査）内容

- （1）防止について
- 　ア　設定に関する知識不足について
- 　　管理者の研修等？、設定の確認
- 　イ　入退室禁止の実態の確認

- （2）発見について
- 　ア　ログの確認
- 　イ　アラートの設定
-

3　委託先の監督について

（1）グループ会社による責任感喪失？

- **→権限明確化**

- **（2）再委託先あることによる管理強化**
- **→B社も、事件後に再委託のガイドライン作成の可能性**
-

4　外部監査依頼の主体

- （内部の対応では無理であったという前提で）外部監査をしていれば、対策ができた可能性が高まると思われるが、どこが主体となって監査の依頼をするか（本件では、Ｂ社かＳ社か）。

→　本件で、B社は、大手セキュリティ外部監視機関と合弁で個人情報を扱うシステム専門の子会社を設立

→　通常は、Ｓ社の依頼によるのではないか（Ｂ社はその有無を確認）。

５　システム管理基準との関係

- **（１）システム管理基準**
- **Ⅶ．外部サービス管理**
- **3.契約と管理**
- **3.2委託先管理**
- **(2) 外部委託元管理者は、契約に基づき、必要な要求仕様、データ、資料等を提供すること。**

- **＜着眼点＞**
- **④ 委託先の情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。**

- (3) 外部委託元管理者は、契約に基づき、委託先より業務報告書に基づく報告を定期的に受けていること。

- ＜着眼点＞
- ② 業務報告書には、委託業務の進捗状況又は稼動状況、品質管理状況、発生した問題点と対策状況、セキュリティ対策の実施状況及び今後の予定等の必要な事項が記載されていること。

- (5) 外部委託元管理者は、情報システム戦略委員会で定めた「委託先に対する立入監査又はモニタリングの実施対象の選定基準」に該当する場合、立入監査又はモニタリングを実施すること。

- ＜着眼点＞
- ① 立入監査等では、契約で取り決めた事項に対する遵守状況、情報セキュリティ管理態勢、事故等(サイバーセキュリティ事案を含む)への対応態勢や再委託先（再々委託先以降も含む）の管理状況等を確認すること。
- ② 委託先において再委託が行われている場合は、契約に基づき、再委託（再々委託以降も含む）先の業務の実施状況を把握すること。

- 4.**サービスレベル管理**(SLM)
- (3) **外部委託元管理者は、外部委託業務が** SLA **を満たしているかを定期的に確認し、その 結果を外部委託元部門長に報告すること。**
- **＜着眼点＞**
- **③ 情報セキュリティに関する合意レベルの維持管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。**

（２）情報セキュリティ管理基準

- 15 **供給者関係**
- 15.1 **供給者関係における情報セキュリティ**
- 15.1.2 **関連する全ての情報セキュリティ要求事項を確立し、組織の情報に対して、アクセス、処理、保存若しくは通信を行う、又は組織の情報のためのＩＴ基盤を提供する可能性のあるそれぞれの供給者と、この要求事項について合意する。**

- 15.1.2.2 特定された情報セキュリティ要求事項を満たすために、供給者との合意には、提供し又はアクセスされる情報の記載、及び提供方法又はアクセス方法の記載を含める。

- 15.1.2.5 特定された情報セキュリティ要求事項を満たすために、供給者との合意には、契約の各当事者に対する、合意した一連の管理策（アクセス制御、パフォーマンスのレビュー、監視、報告及び監査を含む。）の実施の義務を含める。

6　監査範囲の問題

たとえば、対象会社の機器の設定まで監査できるのか？

ｅｘ．ヒアリングをして、「設定に問題ありません。」との回答があったにもかかわらず、実態確認ができるのか。

→通常は、困難ではないか。

それでも、結果が発生してしまった場合には、監査人の責任が問われる可能性がある。

契約で監査の範囲（深さ）を明確にし、監査人の責任を限定しておくべき。

- お時間を頂き、ありがとうございました。