判例評釈　ベネッセ事件地裁判決

東京地裁立川支判平成28年３月29日、
ＴＫＣ判例データベース <LEX/DB25543202>。
東京地裁立川支部平成26年（わ）第872号・第971号、
不正競争防止法違反被告事件。

帖　佐　　隆

１．事案の概要

Ｙは、通信教育、模擬試験の実施等を業とするＰ社（株式会社ベネッセコーポレーション）がＱ社（株式会社シンフォーム）に対し業務委託していたＰ社の情報システムの開発等の業務に従事し、Ｐ社及びＱ社が秘密として管理する（＝争いがある）とするＰ社の顧客の氏名、生年月日、住所等の事業活動に有用な営業上の情報（顧客情報）であって、公然と知られていないものを、同情報が記録されたＰ社のサーバコンピュータに業務用パーソナルコンピュータからアクセスするためのＩＤ及びパスワード等を付与されるなどして、Ｐ社及びＱ社から示されていた者である。

第一の起訴事実として、Ｙは、営業秘密の管理に係る任務に背く形で（＝争いがある）、かつ、不正の利益を得る目的で、Ｑ社内の執務室において、同社から貸与されていた業務用パーソナルコンピュータを操作してＰ社の顧客情報等が記録されたサーバコンピュータにアクセスし、１００９万２０８７件の顧客情報のデータをダウンロードして前記パーソナルコンピュータに保存した上、前記パーソナルコンピュータとＵＳＢケーブルで接続した自己所有のスマートフォンの内蔵メモリに前記顧客情報のデータを記録させて複製を作成する方法により、営業秘密記録媒体である前記サーバコンピュータに記録されていたＰ社の営業秘密である顧客

情報を領得し、その後、インターネットカフェにおいて、同所に設置されたパーソナルコンピュータと前記スマートフォンをＵＳＢケーブルで接続し、前記パーソナルコンピュータを操作して、インターネット上の大容量ファイル送信サービスを使用し、同サービスに係るサーバコンピュータに、前記の方法により領得して前記スマートフォンの内蔵メモリに記録されていた１００９万２０８７件の顧客情報のデータをアップロードした上、名簿業者に対し、前記データを前記サーバコンピュータからダウンロードするためのＵＲＬ情報等を電子メールで送信し、前記ＵＲＬ情報を利用して前記サーバコンピュータにアクセスした前記名簿業者の代表者に、同人が使用するパーソナルコンピュータに前記データをダウンロードさせて記録させることにより、Ｐ社の営業秘密である顧客情報を開示したものである。これについては、不正競争防止法２１条１項３号ロ(注1)、及び２１条１項４号に該当するとして起訴されている。

第二の起訴事実として、Ｙは、営業秘密の管理に係る任務に背く形で（＝争いがある）、かつ、不正の利益を得る目的で、前記Ｑ社執務室において、同社から貸与されていた業務用パーソナルコンピュータを操作してＰ社の顧客情報等が記録されたサーバコンピュータにアクセスし、１９８０万９０５件の顧客情報のデータをダウンロードして前記パーソナルコンピュータに保存した上、前記パーソナルコンピュータとＵＳＢケーブルで接続した自己所有のスマートフォンに挿入したマイクロＳＤカードに前記顧客情報のデータを記録させて複製を作成する方法により、営業秘密記録媒体である前記サーバコンピュータに記録されていたＰ社の営業秘密である顧客情報を領得したものである。これについては、不正競争防止法２１条１項３号ロに該当するとして起訴されている。

そして、上記、第一の起訴事実に係る罪と第二の起訴事実に係る罪とは併合罪にあたるとされるところである。

Ｙは、上記各行為について、自己の行った開示・複製等の行為や図利加害目的等について認めているが、①営業秘密性のうち秘密管理性の要件、

②営業秘密の管理に係る任務に背いて、とする要件の二点について、Ｙは争っている。

２．判旨

有罪判決。

懲役３年６月及び罰金３００万円（実刑）。

（１）秘密管理性について

「秘密管理性の要件は…法益保護の観点から保護に値する情報を限定するとともに，当該情報を取り扱う従業者に刑事罰等の予測可能性を与えることを趣旨として設けられた要件であると解される。このことからすれば，前記要件のうち『秘密として管理されている』といえるためには，①当該情報にアクセスできる者を制限するなど，当該情報の秘密保持のために必要な合理的管理方法がとられており，②当該情報にアクセスした者につき，それが管理されている秘密情報であると客観的に認識することが可能であることを要する。もっとも，それを超えて，個人情報等の重要情報に関して議論されている，外部者による不正アクセス等の不正行為を念頭においた，可能な限り高度な対策を講じて情報の漏出を防止するといった高度な情報セキュリティ水準まで要するものとはいえない。」

「本件当時，本件データベースのデータにアクセスする権限を与えられていたＱ社の従業者は少なくとも１６５名であり，これは同社の従業員総数の約１４パーセントにもなるが，Ｑ社が主にＰ社のシステム開発等を行うグループ会社であり…その作業のために多くの従業者にアクセス権限が与えられていることも当然のことであり，前記アクセス権限者の人数をもって，本件顧客情報にアクセスできる者が限定されていないとはいえない。」

「本件顧客情報については，秘密管理性の要件を充足しているというべきである。」

（２）任務違背要件について

「不正競争防止法２１条１項３号及び４号の営業秘密の管理に係る任務とは，営業秘密を保有者から示された者が，保有者との間の契約等によって課せられた秘密を保持すべき任務をいう。」

「本件において，Ｑ社社員とＹとの間に直接の指揮命令関係があったとは認められず，他にそれをうかがわせる事情も認められないから，ＹのＱ社多摩事業所における勤務実態が，実質的な労働者派遣であり，いわゆる偽装請負であったということはできない。」

「Ａ社・Ｂ社間及びＢ社・Ｃ社間の各業務委託契約においても無効とすべき事情は認められない。」

「Ｙは，本件顧客情報の保有者たるＰ社及びＱ社に対し，本件顧客情報の複製や第三者への開示をしてはならない旨の秘密保持義務を負っており，その旨認識していたにもかかわらず，その義務に違背したものであると認められる。」

３．判決への賛否

結論反対。

少なくとも、営業秘密性（秘密管理性）を充足しないとして、無罪とすべきである。

４．秘密管理性について（評釈）

（１）秘密管理性の趣旨と一般的解釈論

本事件においては、争点の一つとして、秘密管理性が挙げられている。よって、まずは不正競争防止法が要求する秘密管理性（同法２条６項）の趣旨について考えてみたい。

①秘密管理性の趣旨

秘密管理性の趣旨としては、大きく分けて二つあるとおもう。

まず、情報とは基本的に無主物であり、情報に触れた者はこれを自由に利用してよいことが原則である。だが、投資や労力をかけた情報は往々にして財産的価値があり、これを保護しないことは、その財産的価値を毀損させ、冒用者を利することになってしまう。これでは知的財産創出へのインセンティブを喪失させてしまい、妥当でない。

そこで、法は、これらを両立させるべく、保有者に秘密を保持するための努力義務を課すことにより、一定の秘密管理体制を要求し、その秘密管理体制を突破する（注2）行為についてのみ法的保護を与えることとしたのだと考えられる。これが第一の趣旨である。

この点、田村善之教授は、「秘密として管理されていないような情報は遅かれ早かれ他に知られるところとなり，企業の優位性は失われることになる」（注3）としたうえで、「法は，法的保護を欲する者に秘密として管理する相応の自助努力を促す」（注4）（注5）ことを秘密管理性の趣旨の一つとしている。

したがって、秘密管理性には、その秘密にしようとする努力のあらわれとして、情報へアクセスする者を制限するなどのアクセス制限の存在が必要となることが理解されよう。

また、秘密管理体制が充分でなければ、上記のとおり、早晩、優位性がなくなるのであるから、この秘密管理性の第一の要件（第一の趣旨）は、秘密情報を保有者の財産たらしめる要件であるともいえよう。

第二の趣旨としては、上述のとおり、情報に触れた者はこれを自由に活用してよいことが原則なのであるから、情報に触れる者にとって、自由に利用してはいけない情報と自由に利用してよい情報を峻別できることが必要となる（注6）。そうでなければ情報に触れる者にとって損害賠償責任等が生じたり刑事罰を科せられたりするなど不測の不利益を被ることになるからである。

したがって、情報に触れる者が、自由に利用できる情報であるかどうかを認識できる状態を作らなければならない。したがって、法は、第三者が自由に利用できる情報かどうかを識別可能とし、この情報に触れる者からみた客観的な認識可能性を担保するために秘密管理性を要求したのだともいえる。

よって、上記のことから、秘密管理性には、情報に触れた者が当該情報を自由に利用できるかどうかの客観的認識可能性の存在が必要となることが理解されよう。

②秘密管理性の解釈論とその二要件

これらに対し、これまでの裁判例や通説における解釈論としての秘密管理性の要件としては、裁判例ごとに若干のばらつきはあるが、①対象情報にアクセスできる者が制限されていること、②対象情報にアクセスした者が当該情報が営業秘密であることを客観的に認識できるようにしていること、の二要件が必要であるという考え方がとられてきた(注7)。この二要件は上記第一の趣旨、及び、第二の趣旨の考え方がそれぞれ反映されたものであると解され、妥当性ある枠組みであるといえよう。本稿では、①について、秘密管理性の「アクセス制限要件」（第一要件）と、②について、秘密管理性の「客観的認識可能性要件」（第二要件）とすることとしたい。

なお、この秘密管理性であるが、外国法においてもそれに類似する保護の要件がみられる。たとえば、米国における統一トレードシークレット法では、「その環境下で、その情報の秘密を保持するために合理的である努力（efforts）の対象であること（the subject of efforts that are reasonable under the circumstances to maintain its secrecy)」を要求している（傍線筆者)(注8)。

また、米国経済スパイ法では、「保有者がそのためにそのような情報を秘密に保つ合理的な措置（measures）をとっていること（the owner thereof has taken reasonable measures to keep such information secret)」（傍線筆者）を要求している(注9)。

つまり、秘密管理性要件（第一要件及び第二要件）は、秘密にする努力を要求することにより保護の意義を実効あらしめ、有用性ある非公知情報を峻別し、保有者の財産として画定せしめる（財産たらしめる）要件であるといえよう。

なお、近年、秘密管理性の解釈として、上記の第一要件（秘密にする努力・アクセス制限要件）が不要であるとの見解が出現してきた[注10]。しかしながら、筆者はこれには賛同しがたい。上記田村教授がいうように、この第一要件がなければ、早晩公知になるのだからである。そして、本来無主物であり、かつ、本来アクセス自由であるはずの情報を保有者の財産であるとはいえなくなるからである。

（２）秘密管理性の規範的説示について

これに対し、本判決では、秘密管理性について、「『秘密として管理されている』といえるためには，①当該情報にアクセスできる者を制限するなど，当該情報の秘密保持のために必要な合理的管理方法がとられており，②当該情報にアクセスした者につき，それが管理されている秘密情報であると客観的に認識することが可能であることを要する。もっとも，それを超えて，個人情報等の重要情報に関して議論されている，外部者による不正アクセス等の不正行為を念頭においた，可能な限り高度な対策を講じで情報の漏出を防止するといった高度な情報セキュリティ水準まで要するものとはいえない」とする。

まず、前段の秘密管理性の解釈に対する規範的説示であるが、概ね妥当であると解される。これは、上記で筆者が述べた秘密管理性の考え方とも一致するし、過去の多くの民事裁判例や、いくつかある刑事の裁判例、そして通説的見解とも整合するからである[注11]。すなわち、筆者の述べた、アクセス制限要件（第一要件）と客観的認識可能性要件（第二要件）とを本判決でも説示しているからである。

これに対して、後段部分がいう「高度な情報セキュリティ水準」の問題については議論の余地はあろう。すなわち、秘密管理性の水準が高くある

べきか低くあるべきかの問題とも結び付く[注12]。これについて、本判決は、そこまでの高度性は不要であると述べていることとなる。

筆者も秘密管理性について、とりたてて高度である必要はないと考える。とはいえ、とりたてて低度でよいとも考えない。秘密管理性要件を実効あらしめる程度の水準が望ましいということになろう。とはいえ、あまりにも高度であることが必要と考えるならば、知的財産の保護として実効を欠くことになろう。したがって、管理のコストと漏洩のリスクを勘案した程度には必要、ということになるのではなかろうか（参考：田村注12文献６号791頁、等)。

翻って、上記説示の後段であるが、たしかに、「それを超えて，個人情報等の重要情報に関して議論されている…高度な情報セキュリティ水準まで要するものとはいえない」という点については、あえて反対であるとまではいえない。営業秘密侵害罪における秘密管理の程度として解釈論としては容認できるといえよう。たしかに、秘密を保持する努力を要するにしても、本事件は内部者による任務違反の類型であるのだから、対・外部者に対する基準よりは緩やかでよいという考え方もあるであろう。

ただ、この説示をいうのであれば、被告人であるＹに、個人情報流出の責任（保有者Ｐ社やＱ社の財産に対する侵害の責任ではない）を営業秘密侵害罪の刑事罰として問うのは誤りではないだろうか。

なお、個人情報の保護（個人情報保護法）との関係の点については後にまた言及することとしたい。

（３）秘密管理性の事実認定について（Ⅰ．アクセス人数）

それでは、次に、本判決における秘密管理性の事実認定について検討したい。

事実認定において、決定的に問題があるのは、「アカウント教示を受けていた者の数」についての認定部分と、これにより秘密管理性ありと判断する部分である。

まず、事実認定では、「本件当時，本件データベースの本番環境用サー

バ又は本番環境用パッチサーバにアクセスする権限を付与されていた者は，Q社の従業者が少なくとも１６５名（従業者総数は約１１４２名），同じくP社の従業者が少なくとも９名（従業者総数は約３０００名程度）の少なくとも合計約１７４名いた」（傍点筆者）とするのである。

これを受けて、裁判所の判断としては、「本件当時，本件データベースのデータにアクセスする権限を与えられていたQ社の従業者は少なくとも１６５名であり，これは同社の従業者総数の約１４パーセントにもなるが，Q社が主にP社のシステム開発を行うグループ会社であり，Q社にとって本件システムの開発が大規模な受託業務であることからすれば，その作業のために多くの従業者にアクセス権限が与えられていることも当然のことであり，前記アクセス権限者の人数をもって，本件顧客情報にアクセスできる者が限定されていないとはいえない。以上のことからすれば，本件顧客情報にアクセスできる者は一定の範囲に限定されていたと認められる」（傍点および傍線は筆者）とし、秘密管理性の充足を認めている。

この説示は明らかに論理矛盾を起こしている。それも判決に触れた者が一見して理解できる論理矛盾である。このアクセスできた人数について、「少なくとも…名」などという認定がなされているのだが、これで、果たして「アクセスできる者」が「一定の範囲に限定」されているといえるのであろうか。

この説示は誤記ではない。また判決書も更正されていない。裁判所が明白な意思をもって「少なくとも…名」と説示しているのである。改めて読者に説明するまでもないが、「少なくとも…名」といえば、「…名以上」という意味なのであり、理論的には無限大まで包含する概念であろう。これがなぜ「一定の範囲に限定」といえるのか。むしろ「限定」とは逆の概念、すなわち、限定がなかったことを事実認定しているのである。その結果、秘密管理性の認定につき、白というべきところを黒というがごとき説示になっているのである。

このような事実認定になぜなったのであろうか。この点、裁判所が予断

をもっており、最初から有罪と決めつけているのではないかとの疑いをもたれても仕方がないであろう。そして、このような説示があると、果たして、公平な裁判所による裁判（憲法３７条１項）が行われているかどうかの疑念も生じてくるところである。

この説示から推測するに、弁護人の弁護活動のいかんにかかわらず、この部分は最初から裁判所の定めたストーリーの中にあり、いわばテンプレート化された形であらかじめこの説示は定められ、かつ予定されていたのではあるまいか。

おそらく、本・刑事裁判の当初は、「アクセスできる者」について、何らかの確定された人数が検察官より主張されており、その場面でこのストーリーが生み出されたのであろう。しかしながら、その後の裁判の進行の結果、「アクセスできる者」の人数が増大し、確定できなくなってしまったのではないだろうか。にもかかわらず、当初のテンプレートをそのまま使用しようとしたがゆえに、このような矛盾が生じたと推測される。これは一見して些細な誤りのように見えるかもしれないが、きわめて重大な問題が含まれているように思われるのである。

そして、本説示によれば、アクセスできる者の人数は、まったく確定できていないのである。つまり、「少なくとも…名」の「…名」というのは、単に判明した人数を述べているだけで、実際に何名いるかはＰ社もＱ社もまったく把握できていないのではなかろうか。その結果、アクセスできる者の人数について何ら立証できておらず、その結果、アクセスの制限は存在しなかったことになるのではなかろうか。

以上のことからすれば、「アクセスできる者」は「一定の範囲に限定」など到底なされていない。この点でまずアクセス制限がないこととなり、秘密管理性はないといえよう。上記説示は、秘密管理性がないことを裁判所が自白するものだと断定せざるをえないのである。

（４）秘密管理性の事実認定について（Ⅱ．アカウント管理手続）

次に、アカウント管理手続について考えておきたい。

判決は、事実認定として、「Ｐ社及びＱ社において本件システム及び連携システムの各データベースに集積されている顧客情報にアクセスするには…アカウント使用の承認が必要であり，個人用，業務用いずれのアカウントについても，新規発番は，当該システムの担当部門の上長である課長が，発番の必要性等を判断し，その上位の部長の承認を受けた上，同部門から発番を担当するインフラ部門に対して申請を行い，発番を受けるという流れで行われていた。この際，インフラ部門がアカウントリストという使用者の一覧表を作成しており，各部門もこれを利用することができた。また，発番済みの業務用アカウントにつき，追加的に新たな従業者に使用させる場合は，各部門の上長が，具体的な業務割当を決定する際に，どの従業者に追加的に業務用アカウントを使用させるかを判断して承認していた。そして，各部門の課長は，要員計画表や業務日報，ＷＢＳと呼称される工程管理表といった各業務に関する資料を通じて，誰がどの業務に関する業務用アカウントを使用しているのかを把握しており，部門によっては，その時々の業務用アカウントの使用者を一覧できる資料を作成しているところもあった。また，顧客分析課においては，Ｓが課長に就任後，前記の一覧できる資料の作成に代えて，発番済みの業務用アカウントを追加で使用することとなった従業者は，個人用アカウントの発番も受けるというルールを設けることで，前記アカウントリストによって一元的に管理するという運用をしていた」と事実認定し、Ｑ社が精緻な手続によりアカウントを発番し管理していた旨をいう。

しかしながら、上記「少なくとも…人」の説示で当該説示はすべて信憑性がなくなっていることに裁判所は気づいているであろうか。

つまり、上記のような発番および管理手続をしているのであれば、アカウントが付与され、かつ、アクセスできる人数が、「少なくとも…名」、つまり不明であるということは断じてありえない。つまり、Ｑ社は、アカウント発番について、一件ずつ、上記説示のような手続きをし、かつ、業務用アカウントの使用状況を把握しているのであれば、アクセスできる人数

は明確に確定できるはずなのである。上記説示はアカウント発行の際の手続やアカウント利用者の把握について、細部にわたり説示しているが、逆に、細部にわたる説示があればあるほど信憑性がなくなっているのである。そのような細部にわたる手続が正しく行われているのであれば、若干の誤差や若干の不明点があるにしても、もう少し具体的で、かつ、それこそ限定されたアクセス可能人数が出てくるはずなのである。にもかかわらず、「少なくとも…名」などという数値しか出てこないのであれば、上記手続は行われていなかった可能性が高いのではないか。

上記事実認定の根拠はどこにあるのであろうか。これがＰ社あるいはＱ社の従業員の証言が根拠であろうか。ともかく「少なくとも…名」とあわせれば、当該部分における裁判所の事実認定には誤りがあることになるのではないか。

そうなると、上記の説示によるアカウント管理の手続はなかったものと考えざるをえず、この点からみてもアクセス制限はないということになる。そうだとすれば、アカウントは管理なく発行されていたことになり、これによりアカウントが有名無実となっている可能性も出てくることとなる。これでは保有者はアクセス制限を課していたとはいえなくなり、また、従業者等にとっての客観的認識可能性もまたないこととなる。

したがって、このことからも、秘密管理性は充足しないと考えられるのである。

（５）秘密管理性の事実認定について（Ⅲ．人数論と共有フォルダの問題について）

次に、人数論と共有フォルダの問題について考えておきたい。

①人数論について

判決は、「本件当時，本件データベースのデータにアクセスする権限を与えられていたＱ社の従業者は少なくとも１６５名であり，これは同社の従業者総数の約１４パーセントにもなるが，Ｑ社が主にＰ社のシステム開発を行うグループ会社であり，Ｑ社にとって本件システムの開発が大規模

な受託業務であることからすれば，その作業のために多くの従業者にアクセス権限が与えられていることも当然のことであり，前記アクセス権限者の人数をもって，本件顧客情報にアクセスできる者が限定されていないとはいえない」とする。

上記説示においては上述した「少なくとも」の問題があるが、これは措くとして、仮に「少なくとも」がなく、人数が１６５名と認定されたとしよう。判決も「約１４パーセント」と述べていることから、その場合について述べていると解される。

そのような形で人数がしっかりと確定されているとしたならば、上記の説示は必ずしも誤りとはいえない。この点では当該説示に賛成である。つまり、真に必要性があれば、人数の多寡は関係がない。この点は妥当である。判決が述べるとおり、必要がある場合はそれらの人数の者に業務を遂行させなければならないのであるから、当然、アカウント発給の人数は多くなる。これをもって営業秘密性が否定されるのは不当であり、したがって、必要があれば、その人数の多寡は関係がないといえよう。ゆえに必要でない者にアカウントを発給していないことが徹底されてさえいれば、発給した人数が多かろうとアクセス制限が存在するということになる。

したがって、上記の説示については、「少なくとも」ではない確定した165名であるとするならば、筆者も妥当であると評価する。

②共有フォルダの問題について

しかしながら、次のような説示がある。

「本件システムの構築作業中，Q社の社内ネットワーク上の顧客分析課の共有フォルダ内には，本件データベースの接続情報や各種アカウント，パッチサーバに自動接続できるマクロファイル等が複数蔵置され，本件システムの開発等の業務担当者が本件システムにアクセスする際に利用していた。」

「また，発番済みの業務用アカウントを新たに使用する従業者は，口頭又はメールで当該アカウントの教示を受け，その際，前記共有フォルダ内の

ファイルの教示を受けることもあった。」

つまり、顧客分析課の共有フォルダ、つまりネットワーク上の共有スペースには、対象情報が格納されている本件データベースへの接続情報（ＩＤ・パスワード、等）があり、アカウントを発給されていない者も本件データベースにアクセスできたというのである。

しかし、このような事実があっても、判決は秘密管理性を肯定する。すなわち、判決は、

「本件当時，前記共有フォルダにネットワーク上アクセス可能だったのは，シンフォーム事業開発部所属の約７４名であるところ，うち顧客分析課所属の約３９名は本件システムのアカウントの使用を許諾されており，本来アクセス権限を有しないにもかかわらず，本件データベース内の顧客情報にアクセスし得たのは約３５名程度であった。また，実際に業務用パーソナルコンピュータから本件データベース内の顧客情報にアクセスするためには，直接アクセスする場合はＦ社のソフトウェアが，パッチサーバを経由してアクセスする場合はテラタームというソフトワェアがそれぞれ必要であり，前記約３５名のうち，各人の業務用パーソナルコンピュータに前記いずれかのソフトウェアが設定されていたのは合計８名であった。」とし、そのうえで、

「本来アクセス権限を有しないにもかかわらず，共有フォルダ内に蔵置されていた本件データベースの接続情報や各種アカウント等にアクセスでき，本件データベース内の顧客情報にアクセスするための必要なソフトウェアが設定されていた者は合計８名であり，本件データベースにアクセスするには，それなりにコンピュータスキルを要すると考えられること等からすれば，本件データベース内の顧客情報に現実的にアクセスできた者は前記８名よりも更に少ない人数であった可能性が高いといえる。したがって，本件システムのアカウントを始めアクセスに関する情報が顧客分析課の共有フォルダ内に複数蔵置されていたという事実を勘案しても，Ｑ社におけるアカウントを用いた顧客情報へのアクセス制限が，その実効性

を失っていたとはいえず，前記秘密管理性の認定を覆す事情とは認められない。」

とするのである。

③評価

しかしながら、これらは妥当でない説示なのではなかろうか。

秘密管理性の面からいえば、その認定に際し重要な点は、Q社が従業員にアクセス制限を課していたかどうかということなのである。この点からいえば、少なくとも、上記顧客分析課においては、対象情報が格納されているデータベースへのアクセス制限を課していなかったことになる。これは秘密管理性を否定する材料であるといわざるをえない。

また、これは、Q社にとって単なる小さなミスと評価できるのであろうか。そうは思えない。前掲の「少なくとも…人」の問題ともあわせて考えれば、Q社にとって、充分にアカウントの管理ができていなかった可能性が高い。すなわち、アカウントが、少なくとも当該部署では有名無実になっていたと評価できよう。

加えて、上記説示では、現実にアクセスできた者、いうなれば、ソフトウェアをインストール等していた者が８名であったことを理由に、秘密管理性を肯定する。しかしこれは大きな誤りではないだろうか。

先に述べたように、判決は上記１６５名の説示の部分で人数論を否定している。にもかかわらず、この８名の部分については、結果としての人数論によって秘密管理性を肯定しているのである。これは明らかに自己矛盾に陥っていないだろうか。判決は、秘密管理性の肯定については人数論ではないとしながら、秘密管理性が不備である点については、自らが否定した人数論を持ち出している。これは矛盾であり、また、誤りをおかしているのではないか。

そうではなくて、少なくとも、Ｙが外部委託業務従事者（＝後述するが、偽装請負要員であるとの争いがあり、実質的には派遣社員であった可能性もある。判決は否定。）として職務を行う顧客分析課においては、当

該データベースサーバに対して誰でもアクセスしようと思えばアクセス可能であったことを評価すべきであろう。

卑近な例でいえば、本判決の事実認定において、データベースに係るサーバをある種の会議室に例えるならば、不必要な者まで入室可能なように、これに入室する鍵が共用スペースにぶらさげられていたようなものである。そして、その例えでいえば、判決は、これに実際に入る準備をしていた者が８名にすぎないから秘密管理性があると述べているようなものである。

しかし、秘密管理性の判断はそうではなかろう。この部分の事実では、やはり、アカウントが有名無実であったこと、その結果、事実上アクセス制限がかけられていなかったということを事実認定し評価すべきであろう。つまり、少なくとも当該部署の関係者に対しては秘密管理性の要件を充足していないと評価すべきなのである。

④評価～客観的認識可能性論の要件から。

加えて、秘密管理性における客観的認識可能性論の要件からみても、上記説示は問題である。

その理由であるが、たとえ、結果としてアクセスできた者は８名であっても、この事実を外部委託業務従事者からみればどううけとれるであろうか。この事実においては、Ｙからすれば、アカウント（ＩＤ・パスワード）は有名無実であると認識するに充分なのではあるまいか。

つまり、形式的にはデータベースサーバにはＩＤ・パスワードが設定してあったが、そのＩＤ・パスワードは共有スペースに掲示してあり、いわゆる正規従業員らがこのＩＤ・パスワードを使いまわして日常的に業務を行っていたということであろう。そうであれば、それを受け取るＹからすれば、ＩＤ・パスワードは形式的なものであり、有名無実であると認識するのが自然であろう。なお、念のためにいえば、「８名」の事実は、事件当時Ｙは認識しえない事実である。

ちなみに、秘密管理性の議論においては、相対的管理論なる議論がされ

ることがある。すなわち、すべての者に対して高水準で管理されている必要はなく、対象者に応じて秘密管理の程度が異なってよく、対象者が秘密と認識される程度の秘密管理があれば足りるとする考え方である。

この考え方は、上述の、最近出現してきた論である、秘密管理性の第二要件のみを考え、上記の第一要件（秘密にする努力・アクセス制限要件）が不要であるとの見解[注13]とも結びつきそうである。すなわち、これらの見解は、全体として秘密管理が不十分なところがあっても対象者に客観的な秘密管理の認識可能性があれば秘密管理性を肯定するというものである。

しかし、そうであるならば、これを逆に考えることも行わなければ適切ではあるまい。仮に、他の部署では相応に秘密管理がなされていたとしても（本事件においては到底そうは思えないところであるが）、対象者の周囲で秘密管理が不十分であり、対象者がＩＤ・パスワードを有名無実と認識し、その結果、秘密管理性がないと認識する状態なのであれば、秘密管理性はなしとしなければなるまい。そして、本事件では、外部委託業務従事者たるＹの周囲（顧客分析課）でそのような状況であったのだから、ＹはＩＤ・パスワードを有名無実と認識するしかないのではなかろうか。よって、本事件におけるＹとの関係でみれば秘密管理性はなしと考えなければならない。

加えて、第一要件不要論（第二要件だけを考える考え方）においても、対象者（Ｙ）が秘密管理を認識できず彼に不測の不利益を与えることになるのだから、そのように評価しないと片手落ちであり、妥当ではないのである。そしてその考え方からみても、本事件では秘密管理性がないということにならざるをえないのではないだろうか。

⑤小括

以上のように考えるならば、この共有フォルダの問題からみても秘密管理性はないと考えるべきである。

（６）秘密管理性の事実認定について（Ⅳ．Ｐ社およびＱ社の管理職従業者の証言等）

①管理職従業者の証言とＹの主張

上記述べたような、アカウントの発番などの本件データベースに対する秘密管理について、判決は、「公判廷におけるＲ，Ｓ及びＴの各供述により認定した」とする。そして、判決は、「Ｒ，Ｓ及びＴの各供述の信用性」の項を設けて、その信用性について論じている。

Ｒ、Ｓ、Ｔはいずれも本件当時、顧客分析課における上長として、本件システムのアカウントの管理を行っていたということであり、ＲはＰ社およびＱ社で、ＳおよびＴはＱ社で、それぞれ本事件に関連するシステム開発に従事していた旨を判決は認める。

この項で判決は、「前記３名の各供述は，本件システムのアカウントの管理方法等について，それぞれの職務上の地位や経験に基づき，具体的かつ詳細な知見を述べており，その内容についても特段不自然な点はない。加えて，前記３名の各供述は，本件システムのアカウントの新規発番時の手続や，発番済みの業務用アカウントの使用者を追加する場合は，担当部門の上長が具体的な業務割当をするにあたって，その必要性を判断して承認しており，業務用アカウントの使用者の管理も具体的業務の進捗管理とともに行っていること等，概ね整合する内容となっており，相互にその信用性を高め合っている。」とする。また、「前記各説明は一応の合理性があるといえ，前記３名が，客観的事実と明らかに齟齬する虚偽供述を積極的にする理由もうかがえないことにも照らすと，前記各捜査段階の供述は，前記３名の公判廷における各供述の信用性を疑わせる事情とはならない。」という。また、判決は、「前記３名の各供述は，施設の管理，パーソナルコンピュータやサーバ等の管理，従業員等への研修等に関し，概ね合致した供述をしており，その内容は具体的で，不自然なところはなく，業務用アカウントのパスワードが２年以上変更されていないことや共有フォルダ内に必要なアカウントや接続情報が蔵置されていたこと等の不利益な

事情についてもありのままに供述していることが認められる。以上によれば，前記１の認定事実に関する３名の公判廷における各供述は，いずれも信用することができる。」とする。これらの点についてはどのように考えればよいのだろうか。

まず、３名の証言に矛盾がないことであるが、これは、別段不思議なことはなく当然ありうることである。それは３名とも同じ会社ないし関連会社の管理職たる従業者であるため、充分に打ち合わせを行うことが可能であるし、所属企業のための証言を行う動機づけがあるからである。それを殊更に、３名の証言が一致するから信憑性がある旨を説示し、弁護側の主張をすべて退け、かかる３名のみの証言をすべて真実であるとして事実認定するのはきわめて不適切なのではなかろうか。

次に、不利な点も含めて供述していることについては、それは単に弁護側による突き崩しによって否定できなくなったからということはありうるのではないか。証人には偽証罪があるのだから、真実でないことは証言できないからである。

だが、偽証罪の点からすれば、証人の証言のほうに信憑性があるとの主張がされるかもしれない。３名の証言も虚偽であれば偽証罪になるわけであるし、反面、被告人質問は偽証罪に問われないからである。たしかに３名とも虚偽の証言はしづらいところである。

この両サイドの主張・証言についてはどのように考えるべきであろうか。

考えるに、このアカウントの発給の問題やサーバのアクセス状況の問題については、Ｙの主張と証人３名の証言は互いに両立しうるのではあるまいか。

つまり、３名の証言はアカウントの発給の問題なのであるから、Ｐ社やＱ社等で定めた、いわゆる建前論でのアカウントの発給の仕方を述べたものにすぎないのではないか。すなわち、Ｐ社やＱ社にアカウント発給のための建前論としての何らかの規程や取り決めが存在するのであれば、３名はその説明を行いさえすれば虚偽ではないこととなる。また、たとえ一人

に対してでもその手続に沿ってアカウント発給を行った事例があればその説明もまた虚偽にはならないのではないか。

しかしながら、当該３名の証言のみでは、その建前論どおりにアカウントの発給等が日々行われているという立証にはなっていないのではないか。また、現実にはアカウントは存在すれども有名無実であるといった社内の実情が仮にあったとしても、そのような実情は不知というように証言すれば偽証罪には問われない（または本当に不知かもしれない）。つまり、３名の証言ではアカウント等の秘密管理について建前論としての取り決め等が社内に存在することは立証されたかもしれないし、彼らがその方法で実際にアカウントを発給した経験があることは立証されたかもしれない。だが、本事件の発生時に、社内のアカウント発給が建前論どおりに実施されていることは立証されているとはいえないのではないだろうか。

以上のことからすれば、３名の証言では、アカウントの秩序ある発給や、アカウントが有名無実ではなく実効性ある形で使用されていることまでは立証されていないのではないだろうか。ゆえにこれら３名の証言では秘密管理性の存在を立証するには至っていないのではないかと筆者は考えるのである。

②関連～刑事訴訟法における立証責任と立証の程度

ところで、刑事訴訟法における立証責任であるが、基本的にすべて検察官にあり[注14]、かつ、その程度は「合理的な疑いを差し挟む余地のない程度の立証」が必要であるとされる[注15]。したがって、本事件の場合、Ｙが、アカウントが有名無実であることを主張したならば、アカウントが有名無実ではなく実効性ある形で使用されていることの立証責任は検察官にあるはずである。したがって、本事件では立証不尽もあるのではなかろうか。

この点、判決には、「Ｙ以外の従業者が一般的にＹの供述するような運用をしていたことを裏付ける証拠は一切存在しない」という説示もあるが、上記の立証の原則からすれば、この説示もまたおかしい。運用がＹの

供述するとおりになっていないことを検察官が立証しなければならないはずである。

つまり、Ｐ社またはＱ社の管理職３名によってアカウント発番の手続等を証言させただけでは、アカウントが有名無実ではないことの立証は不十分なのではないか。

したがって、この点の立証不尽という観点からみても、秘密管理性の要件は充足しないと筆者は考えるところである。

この点、上記説示では、従業者たるＹのほうから積極証拠を出せ、ということであろうか。しかしながら、上述したとおり刑事訴訟法の立証責任の趣旨とは異なるし、Ｙは相当期間にわたり身柄をとられているわけである。加えて、民事訴訟と異なり、強制捜査の権限が検察官にはある。このような状況の中で民事訴訟と同程度の立証で足りるとするならば、あまりにも被告人たるＹに不利なのではないだろうか。この点、刑事訴訟手続の基本原則から考えても、本判決の説示は妥当でないといわざるをえない。

③関連～営業秘密侵害罪の刑事訴訟における問題点

加えて、この点は、営業秘密侵害罪に係る刑事訴訟（ときに営業秘密事件に係る民事訴訟）における問題点を浮き彫りにしていると思われる。

つまり、営業秘密侵害罪では、秘密管理性の立証、またはその他のいくつかの要件について、被告人側（従業者側）から証拠を提出して積極反証することはきわめて難しいという問題があるのである。保有者側（使用者側）に証拠が偏在しているからである。そして、企業内の問題の場合、証人も当該使用者企業内で働く者がほとんどとなることから、被告人側（従業者側）の証人の出廷も期待できない。また、民事・刑事の営業秘密保護法制（不競法２条１項および２１条１項～とくに２１条１項３号）によって事前に証拠を持ち出しておくこともできないのである。その持ち出しだけで営業秘密保護法制違反ととられる危険性があるからである[(注16)]。この点からみても、上記「合理的な疑いを差し挟む余地のない程度の立証」という立証の程度は営業秘密侵害罪においては特に徹底されなければならな

いのではないか。

にもかかわらず、検察側の立証の程度が低く、なおかつ、Y側に民事訴訟と同程度の立証責任を求めることは、不適切かつ不公平な刑事裁判となるように思われる。

この点、営業秘密侵害罪における刑事訴訟全般の問題として指摘しておきたいところである。

（7）小括

以上の観点からすれば、本事件において秘密管理性を充足すると認定した判断は誤りではないかと思量される。本事件において営業秘密性は充足せず、結果、無罪判決が相当であるのではないかと筆者は考えるところである。

5．任務違背要件について（評釈）

（1）任務違背要件の趣旨と一般的解釈論

次に、本事件において被告人及び弁護人は不競法２１条１項３号、および４号に規定される任務違背要件について争っている。この任務違背要件について次に検討したい。

不正競争防止法２１条１項３号は、「…その営業秘密の管理に係る任務に背き…営業秘密を領得した者」を処罰するが、その中で今回は３号ロの「複製を作成」したことが問題となっているのであるから、本事件における３号の任務違背要件は、Yに複製を禁ずる任務が課せられ、Yがこれに違背したことが必要となる。

また、不正競争防止法２１条１項４号は、「…その営業秘密の管理に係る任務に背いて前号イからハまでに掲げる方法により領得した営業秘密を…その営業秘密の管理に係る任務に背き…開示した者」を処罰するが、任務違背要件が２つあることに留意すべきである。４号前段の任務違背要件は３号の任務違背要件と同じ意味になり、本事件の場合は、Yへの複製を

禁ずる任務がこれにあたる。４号後段の任務違背要件は（使用又は）開示に対応するものであるから、いわゆる秘密を保持する義務となる。

このような任務違背要件であるが、いわゆる秘密保持義務違反だけではなく、あえて３号及び４号前段に規定している以上、別途、複製（等の）禁止の義務が明確に存在しなければならない。加えて、２１条１項は故意犯なのであるから、これらの義務をＹが明確に認識していなければならないことになる[(注17)]。

３号及び４号に問う場合、この任務違背要件が充分検討されていないことが多いように思われる。また、３号ならびに４号前段、及び４号後段の任務違背要件の内容の相違がしっかり理解されていなければならない。３号では複製（等の）禁止の任務が、４号では複製（等の）禁止の任務と秘密保持の任務がそれぞれしっかりと課されていなければ罪には問えないのである。この点、それぞれをしっかり立証する必要があるのである。

また、これらの義務は、社会通念といった概念や、黙示の義務等では足りないと解されるのである。対象者に明示で示されなければならず、かつ、しっかり認識されていなければならないのである。とりわけ、複製禁止の義務については、従業者の使用者に対する忠実義務や一般常識や社会通念といったものからも必ずしも導き出されないのである。それだけに義務はしっかりと明示で示され、対象者も認識している必要があるのである。

（２）本事件における説示等

この点、本事件においては、「不正競争防止法２１条１項３号及び４号の営業秘密の管理に係る任務とは，営業秘密を保有者から示された者が，保有者との間の契約等によって課せられた秘密を保持すべき任務をいう。」とする。この説示について異論まではないが、３号及び４号前段、そして４号後段の任務違背の内容を真に理解しているのかどうかは気にかかるところである。

そのうえで、本判決は、「被告人は，本件顧客情報の保有者たるＰ社及

びQ社に対し，本件顧客情報の複製や第三者への開示をしてはならない旨の秘密保持義務を負っており，その旨認識していたにもかかわらず，その義務に違背したものであると認められる。」と結論付け、３号、４号前段及び４号後段の任務違背要件をいずれも充足しているとするのである。

（３）問題点

しかし、本事件には特有の問題点があるように思われる。判決文によれば、YはQ社のではなく（またA社のでもB社のでもなく）、C社の従業者なのである。そして、C社はB社との間に、システムエンジニアリング業務等に関して業務委託基本契約を締結していて、C社とB社の間で、YをA社の指定場所において、本件システムの開発等の業務に従事させる内容の個別契約を締結していたとする。

また、A社は、システム開発業務及びそれに付帯する業務に関して、B社との間で業務委任基本契約及び機密保持契約を締結しており、B社とA社の間で、Yを、A社の指定場所において、本件システムの開発業務に従事させる内容の個別契約を締結していたとする。

そして、Q社は、A社との間で業務委任基本契約を締結しており、本件システムに関するP社からの委任業務の一部については、A社と業務委任個別契約を締結して、具体的な業務委任をしていたとする。つまり、YはQ社からみて“ひ孫受け会社”の従業者であると認定しているのである。

そして、これら契約は労働者派遣契約でないことは判決も認めている。そうなると、本件事案では、Q社からYへの直接の指揮命令系統はない、ということになる。判旨全体からみれば、このこともまた判決は認めているといえる。

以上の点からみて、まず秘密管理性の点でも疑問が残る。重要な情報であるとする非公知情報を扱う現場で直接の指揮命令系統のない者が日常的に業務を行っていたとなれば、果たしてこれを秘密管理する意思がQ社にあるのかどうか疑わしくなるのではないだろうか。

次に、２１条１項３号および４号の任務違背は、保有者との関係での

「任務」でなくてもよいか、という問題もあるように思われる。すなわち、Q社がYに対して指揮命令することができないのであるから、Q社からYへ直接的に複製禁止義務や秘密保持義務を課すことができないことになるのではないだろうか。たしかに判決文がいうようにYの所属するC社の就業規則やC社との誓約書によって、関係先の業務についても一般的な秘密保持義務はあるようには思われる。しかしながら、それは、Q社に対する秘密保持義務ではないように思われる。Q社の秘密を保持することは、C社に対する秘密保持義務にすぎないのである。本判決の規範的説示も、「営業秘密の管理に係る任務とは，営業秘密を保有者から示された者が，保有者との間の契約等によって課せられた秘密を保持すべき任務をいう」（傍点筆者）としているのだが、保有者たるQ社とYの間では指揮命令系統はないし、保有者との契約等はないことになるのではないだろうか。ここでいう「等」が何を指すのか不明であるが、秘密保持義務は保有者との関係での任務ではないということになるのではないだろうか。そしてその場合に、３号及び４号の適用はありうるのだろうか。これは１つの論点たりえよう。

さらにいえば、Yに、仮に何らかの秘密保持義務があることは予定されているとして、Yには、真に、複製禁止の義務が存在したのであろうか。この点、判決は、「Yが行っていた業務の内容，本件顧客情報の性質及び前記各契約の趣旨からすれば，秘密保持義務の具体的内容として，顧客情報の複製や第三者への開示をしてはならないことを含んでいることは明らかであり，Yにおいてもその旨認識していたと認められる」とする。

たしかに、各社間の委託契約（Yは契約当事者ではない）においては、複製禁止が述べられているようである。これに対し、YがC社に出した誓約書には、「会社及び会社の顧客の機密情報並びに個人情報」の「資料の持ち出し，同情報の複写，複製を行わないこと」等の誓約書を提出したというが、Q社はC社の「顧客」にあたるのであろうか。“ひ孫受け”関係にある以上、厳密な解釈をすれば、あたるかどうか疑わしいということ

になるのではないか。たしかに社会通念という考え方を入れれば該当するとする解釈にもっていくことは可能であろう。しかし、複製禁止義務については、各社まちまちであるため、これを社会通念で規制してよいのか、また、Ｙに本当に故意が成り立っているのか、疑問が残る。結果、当事者（Ｙ）に不測の不利益が生じていることはないだろうか。

加えて、今回のＹの就業形態が、労働者派遣ではなく、偽装請負（偽装委任を含む）だったのではないかとの弁護人の主張も裁判所は退けていて、ＹやＱ社そしてＡ社、Ｂ社、Ｃ社をめぐる秘密保持義務等に関する諸契約は有効ということになった。だが、このＹの就業形態についても、厳密にいえば、労働法規に適合していたのであろうか[注18]。ここにも疑問が残る。たしかにＹの行為に道義的な問題はあろうが、これをとりまくＱ社をめぐるＹの労働に関するそれぞれの委託契約も営業秘密を取り扱うにしては杜撰な契約であるし、任務違背をめぐる諸契約についてもそれが適式にＹに複製禁止義務等を生じさせているかという点で疑問が残るのではあるまいか。そしてそれによって刑事罰を科すことまでを行うには疑問が残る。

以上のように、任務違背要件、すなわち、複製禁止の義務と秘密保持の義務を判決は認定しているが、本事件における諸状況を考えると、特に複製禁止の義務について、疑問なしとはしない。また、このような杜撰ともいえる契約関係でＹが就業を行っていたということからすれば、これは秘密管理性の判断にも影響を及ぼしうることなのではないだろうか。

６．個人情報保護法との関係

（１）営業秘密侵害罪と個人情報保護法、その処罰。

また、本事件を検討するに、個人情報保護法との関係が気になるところである。

思うに、今回、世論は、Ｙに対し、相応の処罰感情があるのが確かにみ

てとれるところである。法律論から若干離れるが、裁判所もそういった世論の処罰感情に配慮して有罪判決（実刑）を宣告したという面は存在するのかもしれない。

しかしながら、その処罰感情は、営業秘密という企業の財産を侵害したところからくるのだろうか、そうではなかろう。この処罰感情は、彼が、個人情報を漏洩したことにあると思われる。ゆえに、この点、有用な技術情報たる営業秘密を不正に使用・開示して利益を得た事例とは処罰感情の質が異なると思われるのである。例えば、東芝・サンディスク事件[注19]といったスパイ行為に強い批判が集まった事件と今回の事件とは同じ営業秘密侵害罪の事件であっても、批難が異質であるのは間違いなかろう。

たしかに個人情報を漏洩したとするＹの行為は容認されるものではない。しかしながら、営業秘密侵害罪は営業秘密という企業の財産を侵害したこと、そして企業がなした成果を冒用したことに対する罪である[注20]。したがって、彼への処罰は保有者企業の財産を侵害したこと及び冒用したことでしか評価できないはずである。

これを前提に本事件をみると、秘密管理性はないと解されるし、本判決では、一応秘密管理性は充足したとされているが、秘密管理の程度が不十分であることは裁判所も認めるところであろう。そうなると、本事件においては企業の財産を侵害したという側面はきわめて小さくなっているといえないだろうか。情報については秘密管理性あってこそ、その財産性を認めることができるからであり、企業が秘密管理をしていない情報について自らの財産だとするのは困難だからである。

これに対し、本判決において、秘密管理が不十分であり、保有企業自身が軽く考えている対象情報、すなわち、当該保有者企業自体が財産として丁寧に扱っていないような情報を、懲役３年６月の実刑プラス罰金３００万円で保護するというのは、営業秘密侵害罪の本旨からすれば、ずれているといわざるをえない。

にもかかわらず、今回、裁判所が厳しい判決を出したのは、個人情報漏

洩に対する懲罰という点からであろう。

しかし、思うに、営業秘密侵害罪は個人情報を保護する法律ではないのである。個人情報の保護は個人情報の保護法制に委ねるべきではないだろうか。

つまり、本判決としては、個人情報漏洩についての処罰を情報財としての財産侵害の罪で代用しているということになる。すなわち、営業秘密侵害罪が個人情報保護のための代用処罰になっているということである。これは妥当でないのではないだろうか。

ちなみに、今回の事件に対し、個人情報保護法の中にＹを処断することのできる罰則はない。ゆえに、営業秘密侵害罪で処断しているのである。しかしながら、筆者は、営業秘密侵害罪は個人情報保護法の代用処罰であってはならないと考えるのである。

（２）個人情報保護法の平成２７年改正

なお、本事件を契機に、個人情報保護法が平成２７年に改正され[注21]、本事件のような事案に対応する罰則が新設された（データベース提供罪。なお本事件には適用不可である。平成２９年５月３０日施行。）[注22]。改正によって新設された個人情報保護法８３条は、個人情報取扱事業者（…）若しくはその従業者又はこれらであった者が、その業務に関して取り扱った個人情報データベース等（…）を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用したときは、一年以下の懲役又は五十万円以下の罰金に処する旨を規定する。

仮に新設された同罪が既に施行されているのであれば、同罪でＹを処断すべきとの議論になることは理解できる（但し、偽装請負（委任）の問題は残る）。しかしながら、筆者からすれば、本事件に適用し、処断する罰則がないがゆえに、秘密管理性の要件その他を無理に合わせこむことにより営業秘密侵害罪を適用しようとしているように感じるのである。これは適切ではなかろう。それぞれの罪は趣旨、保護法益および適用要件が異なるのであるから、無理に合わせこむことはあってはならないと考えるので

ある。

加えて、同罪の最高刑を注目されたい。「一年以下の懲役又は五十万円以下の罰金」なのである。ここでは営業秘密侵害罪との最高刑の差に注目されたい。営業秘密侵害罪の最高刑は十年以下の懲役又は二千万円（本事件当時は一千万円）以下の罰金または併科なのであるから、懲役刑の最高刑でみれば１０分の１にすぎないのである。つまり、世論の処罰感情は理解できるとしても、立法者その他関係者サイドの量刑相場感覚としては、個人情報漏洩の量刑相場はこの程度であると考えられているのである[(注23)]。もっとも、それが立法論的に適切であるかどうかは議論があるところではあろう。

しかしながら、本事件を受けてできた処罰規定の最高刑が一年の懲役又は五十万円の罰金であるのに対し、秘密管理性に疑義のある本事件が懲役三年六月の実刑と三百万円の罰金の併科となるのではあまりにも量刑が過大なのではあるまいか。

この点、営業秘密侵害罪は技術的営業秘密侵害を基準に考えられているがゆえに両罪の間で最高刑に大きな差があるのかもしれない。よって、営業秘密侵害罪の量刑の程度については、技術的営業秘密と顧客情報的営業秘密との間でも充分に検討されなければならない問題であろう[(注24)]。

７．その他の問題

（１）特別法と定義とファービー人形事件

本事件における営業秘密侵害罪は特別法として位置づけられる不正競争防止法に規定されているものである。そうであるならば、この特別法で規定されている保護対象すなわち定義規定を充足しないものは保護されるべきではない。特別法はその法目的のため、その法が要求する保護対象を保護するものだからである。不正競争防止法における営業秘密の定義規定についても同様のことがいえるであろう。そして、まさに営業秘密の秘密管

理性要件についても「完璧な管理である必要まではないが、余りにずさんな管理状態で差止めや刑事罰を認めることは難しいのではなかろうか」ともいわれる[注25]。

民事の事案においては、こういった定義規定を充足しないとして、しばしば請求棄却がなされる。不正競争防止法における営業秘密の案件でもまさにこの秘密管理性がないとして請求棄却となる事例は多数あるし、著作権法の分野でも著作物性なしとして、請求棄却となる事例は多い。

ところが、刑事規定になると、このような定義規定を充足しないとして無罪判決となるのが少なくなる傾向はないだろうか。一旦起訴されているがゆえになかなか日本の刑事司法において無罪判決が出にくいということはないだろうか。

これに対し、著作権法の分野ではあるが、知的財産法の分野であり、ファービー人形事件[注26]の事例を参考にすべきところではないだろうか。同事件では、ファービー人形の偽物商品（無断複製商品）を販売した者らが著作権侵害罪の容疑で起訴されたが、ファービー人形は著作権法上の著作物に該当しないとして無罪判決が宣告されたところである。

同事件でも、事件当初はその被告人らに相当の批判があったと推測される。したがって世論の処罰感情も相応に存在したと思量される。加えて、この事例では、応用美術における著作物性の解釈について、ファービー人形にも著作物性があると解釈する論者も相当数あったと思われ、このような論者の考え方を根拠に有罪判決とすることも可能であったように思われる。しかしながら、同事件では、罪刑法定主義、刑事罰の謙抑性といった観点からもみて無罪判決としたのだと思われる。

同事件も本事件も被告人は実行行為については認めており、そういった実行行為を認定する中、無罪判決は出しにくいのかもしれない。しかしながら、定義規定により無罪となった上記事件を参考にすべきであり、本事件では秘密管理性に疑義があると思量されるわけであるから、むりやり秘密管理性の要件にあわせこもうとはせずに、無罪判決を宣告すべきなので

はあるまいか。そして、本事件では適用不可能であるが、今後起きる同様の問題については新設された上記個人情報保護法８３条で対応すべきなのではなかろうか。

（２）民事と刑事の秘密管理性の逆転現象

また、本判決をみるに、民事と刑事の秘密管理性の逆転現象の懸念がある。民事と刑事では秘密管理性の法文は同じであるのであるから、同等の程度であると考えるのが一般的であり、また、同等の程度であることに問題はない。

しかしながら、立証の程度については、刑事規定なのであるから、より精緻なものが求められるように思われる。また刑事では、立証責任は検察官にあり、加えて、立証の程度は合理的な疑いを入れない程度まで立証しなければならないはずである。したがって、検察官により民事よりも精緻な立証が求められるはずである。

にもかかわらず、本判決は、事実上、アクセス制限をどのように課し、アクセス管理が充分であるかどうか不明であるにもかかわらず秘密管理性ありとしている。これでは通常の民事訴訟の案件よりもきわめて低い管理水準で秘密管理性ありとされているのではないだろうか。

加えて、他の営業秘密侵害罪における刑事事件をみても、ぱちんこ還元率事件[注27]で、秘密管理性の程度がきわめて低いように思われる。このように刑事の案件のほうに秘密管理性に疑義のある事例が散見され、結果、秘密管理性の水準に民事刑事の逆転現象が起きてはいないだろうか。

思うに、刑事裁判においては一旦起訴されると無罪となる確率がきわめて低く、また、世論による批判といった背景などもあるせいか、実際の実行行為が存在する事案については、特別法の入口であるはずの定義規定に疑義があってもこれを理由に無罪とすることは行われにくい傾向にあるようにも思量される。

しかしながら、上述のとおり、特別法における定義規定は意義あるものであり、これを軽視するのでは罪刑法定主義にも反しよう。したがって、

定義規定の充足というのはしっかりとした形で審理され、説示されるべきであるように思われるところである。

（３）裁判所による強い予断

さらに、本判決は、上述した「少なくとも…人」との説示があったり、３人のＰ社およびＱ社関係者の証言の信憑性を殊更に高く評価したりするなど、筆者は、裁判所による強い予断を感じるのである。本事件では、裁判所による予断が排除されないまま判決に至っているのではないだろうか。

本稿では、判決文から受け取れる矛盾について述べたが、このような予断がみられることからみれば、本判決では、他の事項も含めて、事実認定に誤りのある可能性が相応にあるのではないだろうか。

刑事訴訟法で起訴状一本主義（同法２５６条６項）がとられるなど、予断は排除して判断されるべきなのは当然であり、この点、留意されるべきであろう。本判決ではその判決内容に適正でない部分を感じざるをえないところである。

８．おわりに

以上の観点からすれば、本事件においては、秘密管理性を充足しないことを理由とする営業秘密性（不競法２条６項）の欠如によって、被告人Ｙは無罪となるべきなのではないだろうか。そして任務違背要件が欠如している可能性もあると思われる（同法２１条１項３号、４号）。

よって判決の結論および理由は妥当でないように思われるところである。

別注

（注１）不正競争防止法21条１項３号の解釈論については、帖佐隆「不正競争防止法二一条一項三号と任務違背・図利加害目的」久留米大学法学　No.74（2016年）39頁に記した。また、同号の「営業秘密」の「領得」については、

帖佐隆「刑法における『領得』概念と無形的な営業秘密の保護」久留米大学法学　No.73　(2015年）１頁に記した。これらも併せて参照していただければ幸甚である。

(注２）「秘密管理体制を突破する」ことを評価するものについて、田村善之『不正競争法概説』（第２版、2003年、有斐閣）329頁。

(注３）田村・前掲注２　328頁。

(注４）田村・前掲注２　328頁。

(注５）同旨　山口厚「企業秘密の保護」ジュリスト No.852 (1986年) 46頁〔51頁〕。

(注６）田村・前掲注２　328頁。

(注７）通商産業省知的財産政策室監修『営業秘密―逐条解説　不正競争防止法』（1990年、有斐閣）55頁（中村稔執筆部分)、経済産業省知的財産政策室編著『逐条解説　不正競争防止法』（平成23･24年改正版、2012年、有斐閣）41頁。

民事事件の裁判例では、知財高判平成26・８・６裁判所ウェブサイト（平成26年（ネ）第10028号)、名古屋地判平20・３・13判時2013号107頁（平成17年（ワ）第3846号)、東京地判平18・７・25裁判所ウェブサイト（平成16年（ワ）第25672号)、東京地判平15・5・15裁判所ウェブサイト（平成13年（ワ）第26301号）その他裁判例の多数が同旨。

刑事事件の裁判例でもヤマザキマザック事件地裁判決＝名古屋地判平26・８・20ＴＫＣ法律情報データベース <LEX/DB25504719>（平成24年（わ）第843号）同旨。

(注８）Uniform Trade Secrets Act §1 (4) (Definitions)

(注９）18 U.S.C Chapter90 §1831-§1839 (Economic Espionage Act of 1996) §1839 (3) (Definitions)

(注10）経済産業省知的財産政策室編『逐条解説　不正競争防止法』（2016年、商事法務）40頁-42頁。

(注11）前掲注７参照。

(注12）秘密管理性の高低について論じた文献に、田村善之「営業秘密の秘密管理性要件に関する裁判例の変遷とその当否－主観的認識 vs.『客観的』管理－」知財管理64巻５号621頁＝６号787頁（2014年)、近藤岳「秘密管理性要件に関する裁判例研究―裁判例の『揺り戻し』について―」知的財産法政策学研究25号（2009年）159頁、などがある。

一方、髙部眞規子「営業秘密の保護」知的財産法政策学研究　Vol.47 (2015年）59頁〔65頁〕では、秘密管理性の高低の議論を意識したコメントであると解されるが、「裁判例は、様々な事情を総合的に考慮して、個別の具体的事案において、妥当な解決を導いている」とし、「裁判例に、時代による傾向といったものがあるわけではない」と断じている。

(注13）経済産業省知的財産政策室編・前掲注10。

(注14）例えば、池田修=前田雅英『刑事訴訟法講義』（第４版、2012年、東京大学出版会）396頁、白取祐司『刑事訴訟法』（第７版、2012年、日本評論社）331頁。

(注15）最一決平19・10・16刑集61巻７号677頁、白取・前掲注14　330頁。

(注16）不正競争防止法21条１項３号によれば、営業秘密を図利加害目的で複製等すれば、使用・開示を伴わなくても刑事罰が科されうる。もっとも図利加害目的がなければ犯罪構成要件は充足しないが、将来の訴訟への証拠にするた

めの営業秘密の複製・持ち出しは、図利加害目的とされるおそれがあり、刑事罰の危険があり、およそ、企業等の従業者等の側からの証拠の保全は不可能である。

この点、「将来の訴訟に備える目的」での証拠の保全は「図利加害目的」に該当しないと考えるべきである。筆者はそのように提唱したい。参照　帖佐・前掲注１「不正競争防止法二一条一項三号と任務違背・図利加害目的」76頁。

(注17) 本要件について、ヤマザキマザック事件地裁判決(*)は、「秘密を管理する任務に背くとは，情報の保有者との間の契約等による秘密保持義務に違背することである。特に，本件各ファイルの複製を作成することが秘密保持義務違反になることを被告人が認識していたことが必要である。」とする。故意犯であるゆえ当然であるが、被告人の認識をしっかり説示している点で妥当であろう。また、ここでは「秘密保持義務」と説示してあるが、同判決では３号について複製禁止の義務を詳細に検討している。複製禁止の義務が明示されている必要があるのは同判決からも読み取れるところである。

（＊）名古屋地判平26・８・20・前掲注７掲出刑事裁判例。

(注18) 労働者派遣法（労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律）によれば、「労働者派遣」とは、「自己の雇用する労働者を、当該雇用関係の下に、かつ、他人の指揮命令を受けて、当該他人のために労働に従事させることをいい、当該他人に対し当該労働者を当該他人に雇用させることを約してするものを含まないものとする」とする（同法２条１号、傍線筆者）。派遣先の指揮命令下で労働させるにはこの契約によることになる。これに対し、請負契約や委任契約に基づき労働者が他人の事業所で労働する場合は、あくまで指揮命令はその他人ではなく雇用関係にある使用者が行うこととなる。にもかかわらず、実際にはその他人（派遣先）が指揮命令を行っているとなると、いわゆる偽装請負の問題が出てくることとなる。

参考　菅野和夫『労働法』（第10版、2012年、弘文堂）252頁以下。

(注19) 東芝・サンディスク事件

地裁判決…東京地判平27・３・９ＴＫＣ法律情報データベース＜ LEX/DB25506161＞（平成26年特（わ）第438号）。高裁判決…東京高判平成27・９・４ＴＫＣ法律情報データベース＜ LEX/DB25541281＞（平成27年（う）第828号）。

(注20) 営業秘密侵害罪の保護法益は、営業秘密の財産的価値という個人的法益と、競争秩序の維持という社会的法益である。ここでいう競争秩序とは、「成果の程度に応じた勝者の決定」がなされることをいうと解される。

営業秘密侵害があった場合、営業秘密の価値が著しく低下するわけであるから、その財産的価値という個人的法益の侵害となる。加えて、営業秘密侵害とは他人の成果を冒用することであり、この成果の冒用が「成果の程度に応じた勝者の決定を歪曲する」がゆえに競争秩序の維持という社会的法益を侵害することになる。

これに対して、個人情報の保護は上記２つと保護法益が異なるし、また、秘密として管理していなければ、営業秘密の価値が低下しても構わないと保有者が考えていると解され、保有者の財産として評価するのが難しくなるため、営業秘密侵害罪として処断するのは難しくなるといわざるをえない。

参考　帖佐・前掲注１「刑法における『領得』概念と無形的な営業秘密の保護」21頁以下、渋谷達紀『知的財産法講義Ⅲ』（第２版，2008年）12頁、小野昌延=松村信夫『新・不正競争防止法概説』（2011年）３頁以下、小野昌延『不正競争防止法概説』（1994年）１頁以下。

(注21) 個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律（平成二十七年法律第六十五号）（平成27年９月３日成立、平成27年９月９日公布）による改正。平成29年５月30日全面施行。

(注22) 同罪については、本事件がきっかけで改正された旨をいい、また、不正競争防止法で営業秘密の定義を充足しない場合等に同罪で処罰をできるようにしたことが趣旨とされている(**)。

（＊＊）瓜生和久編著『一問一答・平成27年改正個人情報保護法』（2015年、商事法務）150頁以下。

(注23) 瓜生編著・前掲注22 154頁によれば、このような法定刑について、個人情報保護法84条の罰則規定や他法令における同種の罰則規定との均衡を考慮した旨をいう。

加えて、同書（同頁）では、「本罪は、氏名や住所等の公になっているような情報のみを不正に提供する場合も含む個人情報一般に関する不正提供罪であり、その不正な提供によって直ちに具体的な被害が発生するおそれが高いとはいえない点で、特殊な情報のみを対象とする番号利用法（個人番号）や割賦販売法（クレジットカード情報）等とは事情が異なるといえます」とし、そのような理由で同罪の法定刑を定めた旨をいう。

本事件でも、その情報の大半は、住所・氏名等の情報であると考えられる。その点は考慮されなければならないだろう。無論、だからといってＹの行為が道義的に是認されるものではないことは付言する。

(注24) 技術的営業秘密は完全に新規なものであり、それ自体きわめて高い付加価値を示すのに対し、顧客情報的営業秘密は、その情報の束が存在することにより、業務の効率化が実現でき付加価値を示す点で意義（有用性）があるものが多い。本件では、対象情報の漏洩件数が多く、情報の束を使用しているため、秘密管理性があれば、営業秘密侵害は免れない。だが、情報の一つ一つを見た場合は公知情報であるともいえ、その付加価値は小さいともいえる。したがって、その差は量刑等においても考慮されなければならないだろう。

なお、このような顧客情報については、一つ一つを使用しただけでは公知情報の使用にすぎないとも考えられ、そのような場合は、情報の束を使用してはじめて営業秘密の使用となると考えられる。本件では秘密管理性が充足されれば後者に該当するが、しばしば、そのあたり誤解がみられるようにおもう。

(注25) 髙部・前掲注12 66頁。

(注26) ファービー人形事件（第一事件～第三事件）

第一事件高裁判決…仙台高判平14・７・９判時1813号145頁（平成12年（う）第63号・著作権法違反被告事件）。同事件原審…山形地判平成12・３・31判例集なし（平成11年（わ）第167号）～※これのみ有罪判決。

第二事件高裁判決…仙台高判平14・７・９判時1813号150頁（平成13年

（う）第177号・著作権法違反被告事件)。同事件原審…山形地判平成13・９・26判時1763号212頁（平成11年（わ）第184号・著作権法違反被告事件)。

第三事件…仙台高判平14・７・９ＴＫＣ法律情報データベース（平成13年（う）第178号・著作権法違反被告事件)。同事件原審…山形地判平成13・10・10ＴＫＣ法律情報データベース（平成11年（わ）第163号・著作権法違反被告事件)。

(注27) ぱちんこ還元率事件

仙台地判平21・７・16、特許ニュース（経済産業調査会）No.12621（平成21年11月６日（金)）２頁（平成21年（わ）第311号・第364号)。

評釈に、帖佐隆「判例評釈『ぱちんこ還元率等』不正競争防止法等刑事事件（不正競争防止法21条１項（営業秘密における刑事罰規定）の適用について)」パテント Vol. 63 No. 6（2010年）29頁、一原亜貴子「不正アクセス行為により取得したパチンコ店の割数及び売上金額等を競合パチンコ店へ開示した行為につき、不正取得後営業秘密開示罪の成立が認められた事例　（仙台地裁平成二一年七月一六日判決)」岡山大学法学会雑誌　60巻３号（2011年）551頁、専田泰孝「不正アクセス行為により取得されたパチンコ店における『割数』等の情報を開示する行為と不正競争防止法の『営業秘密』侵害罪」高橋則夫=松原芳博編『判例特別刑法 第２集』(2015年，日本評論社）187頁、がある。これら評釈において、同事件では、専田は秘密管理性を充足する旨をいうが、一原は秘密管理性に疑義ありとし、帖佐は秘密管理性及び有用性に疑義あり、とする。