【判例評釈】

不正競争防止法2条6項の「営業秘密」における秘密管理性
――東京高判平成29年3月21日・判タ1443号80頁――

弁護士、甲南大学法科大学院特別講師　黒根祥行

■ 事案の概要

被告人は、通信教育・模擬試験の実施等を業とする株式会社Aが株式会社Bに対し業務委託していたAの情報システムの開発等の業務に従事していた（BからC、D、Eと順次システム開発等の業務委託契約が締結されており、被告人は、Eの社員であった）。

被告人は、A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が記録されたA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A及びBから示されていた。被告人は、平成25年7月頃、所有するスマートフォンを業務用パーソナルコンピュータにUSBケーブルで接続したところ、業務用パーソナルコンピュータからスマートフォンへのデータの書き出しが可能であることに気付いた。それ以後、被告人は、顧客情報を自己のスマートフォンに書き出し、名簿業者に売却するようになった。

本件は、そのような被告人が、不正の利益を得る目的で、その営業秘密の管理に係る任務に背いて、①平成26年6月17日、B事業所執務室において、B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A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Aの営業秘密である顧客情報を領得し、②平成26年6月18日、インターネット上の大容量ファイル送信サービス「データ便」を使用し、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てAの営業秘密である顧客情報を開示し、③平成26年6月27日、前記B事業所執務室において、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A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Aの営業秘密である顧客情報を領得したという不正競争防止法違反の事案である。

原審（東京地立川支判平成28年3月29日判タ1433号231頁）においては、①被告人が複製、開示した顧客情報が、不正競争防止法における「営業秘密」に該当するか、より具体的には、営業秘密の要件の一つである「秘密として管理されている」といえるか（秘密管理性）、②被告人は、本件顧客情報の保有者又は管理者であるA及びBに対して、営業秘密の管理に係る任務を負っていたといえるかが争点となったが、秘密管理性、営業秘密の管理に係

る任務違背ともに肯定され、懲役3年6月及び罰金300万円に処せられた。これに対し、控訴がなされ、控訴審では、一部原審の事実誤認を認めたものの、結論としては有罪とし、量刑不当の点から原審を破棄し、懲役2年6月及び罰金300万円に処した。

■ 判旨

1　秘密管理性について

「所論は、Aが、大量の個人情報を管理して営業に活用している業界最大手の著名企業であり、内部者による侵害行為に対して、容易に対策をとることができることからすれば、秘密管理性があるというためには、原判決が説示する合理的管理方法では足りず、相当高度な管理方法を採用し、実践することが必要であると解すべきであると主張する。

しかし、不正競争防止法2条6項が保護されるべき営業秘密に秘密管理性を要件とした趣旨は、営業秘密として保護の対象となる情報とそうでない情報とが明確に区別されていなければ、事業者が保有する情報に接した者にとって、当該情報を使用等することが許されるか否かを予測することが困難となり、その結果、情報の自由な利用を阻害することになるからである。そうすると、当該情報が秘密として管理されているというためには、当該情報に関して、その保有者が主観的に秘密にしておく意思を有しているだけでなく、当該情報にアクセスした従業員や外部者に、当該情報が秘密であることが十分に認識できるようにされていることが重要であり、そのためには、当該情報にアクセスできる者を制限するなど、保有者が当該情報を合理的な方法で管理していることが必要とされるのである。

この点について、原判決は、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と並んで、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いることを秘密管理性の要件とするかのような判示をしている。しかしながら、上記の不正競争防止法の趣旨からすれば、②の客観的認識可能性こそが重要であって、①の点は秘密管理性の有無を判断する上で重要な要素となるものではあるが、②と独立の要件とみるのは相当でない。原判決の判示は、上記のような趣旨にも理解し得るものであるから、誤りであるとはいえない。そうすると、所論がいうように、Aが、本件顧客情報へのアクセス制限等の点において不備があり、大企業としてとるべき相当高度な管理方法が採用、実践されたといえなくても、当該情報に接した者が秘密であることが認識できれば、全体として秘密管理性の要件は満たされていたというべきである。

これを本件についてみると、原判決が認定するとおり、Bでは、毎年、従業者全員を対象とした情報セキュリティ研修を実施し、個人情報や機密情報の漏えい等をしてはならない旨記載された受講報告書のほか、個人情報及び秘密情報の保秘を誓約する内容の同意書の提出を求めていた上、本件システムの内容及び目的並びにその中の情報の性質等から、本件データベース内に集積される本件顧客情報がAの事業活動に活用される営業戦略上重要な情報であって機密にしなければならない情報であることは容易に認識することができたといえる。そうすると、後記のとおり、本件顧客情報へのアクセス制限に様々な不備があったとはいえ、一定のアクセス制限の措置がとられていたことを併せ考慮すると、本件において、秘密管理性の要件は満たされていたということができる。したがって、本件顧客情報について、秘密管理性の要件が満たされていたという原判決の判断は、結論において正当である。所論は理由がない。」

2　営業秘密の管理に係る任務違背について

「被告人は、Eに対し、機密情報を会社の許可なく外部に持ち出さない旨の誓約書を提出していたこと、Eの就業規則（56条）上、従業員が職務上知り得た機密情報について、秘密保持義務を負ってい

たこと、前記の各社間で取り交わされた業務委託契約には、機密情報に関する秘密保持条項が含まれていたことに照らすと、被告人がEに対して負っていた秘密保持義務の対象としては、被告人がBの業務上取り扱っていた機密情報も含まれると解される。しかし、このことから、当然に、被告人が契約当事者としてBに対して本件顧客情報に関する秘密保持義務を負うことにはならないというべきである。もっとも……BとC、CとD、DとE間の各業務委託契約は、いずれも偽装請負に該当し、被告人は、Bの指揮命令を受けて業務に従事する者であったことから、労働者派遣法2条2号にいう派遣労働者に当たると認められ、同法40条の6第1項1号の類推適用（同条項は、本件当時未だ施行されていなかったが、その趣旨は、本件当時においても妥当するというべきである。）により、被告人とB間には直接雇用契約が成立したものとみなされ、同法24条の4により、業務上取り扱ったことについて知り得た秘密を他に漏らしてはならない義務を負うことになると解するのが相当である。そうすると、被告人は、Bに対して、同社の業務に従事中に知り得た機密情報を外部に漏えいしないことを遵守する旨の同意書を提出しているところ、これは同社との秘密保持契約として有効であり、被告人は、Bに対して、業務上取り扱った秘密について秘密保持義務を負っていたと認められる。前記のとおり、本件顧客情報は、Bの社内規程により機密情報とされ、これに接する者が秘密情報であると容易に認識することができたことに照らすと、被告人は、同社に対して、本件顧客情報について秘密保持義務を負っていたと認められる。」

「なお、原判決は、被告人が、Aに対しても、同様の秘密保持義務を負っていたと判断している。しかしながら、AとBの間に業務委託契約に伴う秘密保持条項があること、及び、被告人がBに対して、本件顧客情報についての秘密保持義務を負うことから、直ちに、被告人がAに対しても直接秘密保持義務を負うと解することはできず、他に証拠もないから、原判決の上記判断は、誤りであるといわざるを得ないが、この点は、原判決の結論には影響しない。」

「被告人は、原審公判において、チームリーダーであるBの社員から指揮監督を受けて、本件システム開発の業務に従事していた旨供述するところ、この供述は、上記の本件システム開発に関する同社の業務形態や被告人の勤務の実情等に照らすと、自然で合理的なものといえる。」

「そうすると、被告人の原審公判供述によれば、被告人は、Bの社員の指揮監督を受けて同社の業務に従事していたと認められるから、同社の社員と被告人との間に直接の指揮命令関係があったことを認めず、BとCとの間等の各社間の業務委託契約が偽装請負に当たらないとした原判決の認定は誤りであるといわざるを得ない。しかし、被告人は、Dの従業員でありながら、Bの社員から直接指揮監督を受けていたことから、被告人が、労働者派遣法2条2号にいう派遣労働者に該当すると認められ、Dが厚生労働大臣の許可を受けずに業として労働者派遣事業を行っていたことが違法と評価されるとしても、このことによって、被告人とB間の雇用関係及び秘密保持契約が、公序良俗に反して無効となるものではない。」

3　量刑について

「原判決が、本件犯行の犯情、すなわち、本件犯行の悪質性、被害者であるAに多大な経済的損害を与えた上、その信用を失墜させるなど、結果が重大であること、本件が連続的犯行の一環であることなどに加え、被告人がシステムエンジニアとして備えるべきモラルを欠いていたこと、犯行の動機が身勝手で短絡的であること、本件犯行の社会的影響や一般予防の必要性等について説示するところは正当であり、被告人の責任が重く、懲役刑の実刑が相当であるとした判断は、首肯し得るところである。しかしながら、既にみたとおり、A及びBには、営業秘密である本件顧客情報の管理等について不備が

多々あり、これらの事情は被害者側の落ち度として、被告人にとって有利な量刑事情に相当するところ、原判決がこれらの点を量刑事情として考慮に入れていないのは、量刑判断として重きに失するに至ったものというべきである。」

「Bにおける本件顧客情報の管理体制については、①本件データベースには、アカウントを通じてアクセス制限が行われていたものの、そのアカウント情報がBの共有フォルダ内に蔵置されていて、閲覧可能であったこと、②私物のスマートフォンの執務室への持ち込みが禁止されていなかったこと、③本件データベースにはアラートシステムが導入されていたが、実際には機能していなかったことなどの点で、不備があったと認められ、これらの点は、本件の発覚後にA社内に設けられた個人情報漏えい事故調査委員会の調査報告においても、指摘されているところである。加えて、前記のとおり、Bにおいては、相当数の業務委託先会社に所属する従業員を、パートナーと称し、実態は派遣労働者として受け入れ、本件システムの開発等の業務に従事させていたものである。特に、被告人は、3次派遣の労働者に該当し、Bの上長においても、被告人の所属先会社を正確には把握していない状態であった。システムエンジニアリングの業界においては、変動する労働力の需要に対応するため、このような安易かつ脱法的な労働力の確保が常態的に行われていたことがうかがえるが、Aのような大手企業が子会社であるBを通じてこのような方法を採り、同社にとって経歴等が詳らかでない者に、経営の根幹にかかわる重要な企業秘密である本件顧客情報へのアクセスを許していたということは、秘密情報の管理の在り方として、著しく不適切であったといわざるを得ない。したがって、A等がこのような労働者に本件顧客情報へのアクセスを許したからには、秘密漏えい対策を講じたとしても、それに伴って生じる危険もある程度甘受すべき立場にあったといえる。また、上記③のアラートシステムについても、これが正常に機能していれば、被告人が同種の情報漏えい行為を行った比較的早い段階で、Bがこれを察知し、更なる被害拡大に対する防止策を立てることが可能であったと思われるのに、アラートシステムが全く機能していなかったため、約1年間にわたって被告人の同種行為が放置され、外部からの通報によりようやく本件が発覚したのであって、被告人が同種行為を反復継続したことが責められるべきであるとしても、被害が拡大したことの原因の一端は、B側の対応にもあるというべきである。」

「被告人が本件犯行に及んだ背景事情として、A及びBにおける本件顧客情報の管理に不備があるとともに、被害が拡大したことの一因として、同社等の対応の不備があると指摘できるのであり、これらの点で、本件における被害者側の落ち度は大きいというべきであって、本件の結果をひとえに被告人の責めに帰するのは相当でないというべきである。」

「原判決は、量刑の理由においてこれらの点に全く言及しておらず、これらの点を考慮することなく前記の刑を量定したものとみるほかない。これらの点は、被告人にとって有利な量刑事情に相当するところ、これらの点を考慮に入れていない原判決は、量刑判断として明らかにバランスを失するものであり、これらを正当に考慮に入れた場合と比較して、重きに失する判断に至ったものといわざるを得ない。」

「したがって、……原判決の量刑は、懲役刑の刑期の点で重すぎて不当であるといわざるを得ない。」

■ 評釈

1　本件の社会的影響

本件は、子供向けの通信教育の最大手企業における大規模な顧客情報流出事件として、当時、マスコミで大々的に報道がなされた事件である。一般家庭の子供の個人情報が大規模に流出したということで、社会的にも大きな問題となり、経済産業省もこの事件を受け、Aに対して報告徴収指示を出し、全国学習塾協会、全国学習塾協同組合、日本通信販売

協会に対して個人情報の適切な管理を強化することなどを要請した。また、A の取締役2名が情報流出の責任を取り、取締役を辞任している。

一審では、懲役3年6月及び罰金300万円、控訴審では、懲役2年6月（実刑）及び罰金300万円の刑が言い渡されている。本件の社会的影響に鑑みれば、実刑は免れないと考えられるが、果たしてこの処罰が重きに過ぎるのか、それとも軽いのか、妥当であるのかは、様々な考え方があるところであろう。また、不正競争防止法の目的は、第1条に記載されているとおり、「事業者間の公正な競争及びこれに関する国際約束の的確な実施を確保するため、不正競争の防止及び不正競争に係る損害賠償に関する措置等を講じ、もって国民経済の健全な発展に寄与することを目的とする」ものである。本件で被告人は、不正競争防止法違反により有罪（実刑）とされているが、実刑とされた主たる理由としては、事業者間の公正な競争の確保というよりは、子供に関する大量の個人情報を流出させ、社会に不安を与えたことに対する制裁と捉えられるのではないかという疑問もある。これらの点については、「4　量刑」で詳述する。

2　秘密管理性

不正競争防止法における「営業秘密」については、同法2条6項に定義規定が置かれており、①秘密として管理されていること（秘密管理性）、②事業活動に有用な技術上または営業上の情報であること（有用性）、③公然と知られていないこと（非公知性）が要求されている。

本件において争点となったのは、このうちの秘密管理性の要件である。

秘密管理性が要求される理由については、ⅰ．行為者（従業員や取引先）に秘密として管理しようとする対象が明確化されることによって、行為者の予見可能性、経済活動の安定性を確保する点から秘密情報の特定とその認識可能性に求める見解と、ⅱ．営業秘密は自己管理が原則であり、営業秘密として保護されるためには適切な管理がなされている必要があるという点から情報へのアクセス制限など合理的管理性に求める見解がある。これら2つの見解は両立しうるものであり、秘密管理性の内容や程度に影響を及ぼすものではないという見解もある[1)]。

秘密管理性の認定にあたって、上記のⅰを重視すれば、情報にアクセスした者に当該情報が営業秘密であることが認識できるようにされていること（客観的認識可能性）が要件として重視され、上記のⅱを重視すれば、情報にアクセスできる者が制限されていること（アクセス制限）が要件として重視されることになる。

秘密管理性が認められるための要件について、民事の裁判例は多数あるが、刑事の裁判例は非常に少ない。民事の裁判例[2)]では、客観的認識可能性とアクセス制限を別個の要件とするものが目立つ。また、従来は、一般的に、客観的認識可能性とアクセス制限の両者が別個の要件として秘密管理性の判断要素として必要と解されていた[3)]。本件の原審においても、両者を別個の要件としており、不正競争防止「法は、事業者の営業上の利益及び公正な競争秩序の維持を保護法益とし、その具体的規定の一環として、刑事罰等による営業秘密の保護を規定していることからすれば、……秘密管理性の要件は、前記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

1）　松村信夫「営業秘密をめぐる判例分析」ジュリ1469号（2014年）33頁。
2）　東京地判平成19年5月31日裁判所 HP、名古屋地判平成20年3月13日判時2030号107頁など。
3）　経済産業省　知的財産政策室編「逐条解説　不正競争防止法　平成27年改正版」（2015年）42頁。

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。」と示している。原審がアクセス制限の点について、「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」と留保をつけた意図は不明であるが、本件で情報管理において不十分な点があることを意識したものである可能性は否定できない。

秘密管理性の認定にあたり、秘密の対象がどういうものであるかを一つのメルクマールにするという考え方も有り得る。秘密の対象が、技術情報であるか、営業情報であるかに分け[4]、技術情報の場合には、有用性の高い情報であることが多いので、従業員にとって秘密保持の必要性や対象となる範囲が明確であるから、営業情報よりも比較的緩やかな管理でも秘密管理性が認められるという考え方も可能だろう。

客観的認識可能性とアクセス制限の両者を別個の要件として判断するかという点について、経済産業省は、平成27年の不正競争防止法改正にあたり、「逐条解説　不正競争防止法　平成27年改正版」において、別個独立の要件ではないと明示した[5]。

すなわち、秘密管理性要件の趣旨を、「企業が秘密として管理しようとする対象（情報の範囲）が従業員等に対して明確化されることによって、従業員等の予見可能性、ひいては、経済活動の安定性を確保することにある」[6]と理解したうえで、客観的認識可能性とアクセス制限は、秘密管理性の有無を判断する重要なファクターであるが、別個独立の要件ではなく，「アクセス制限」は「認識可能性」を担保する1つの手段と考えたのである。

本判決は、秘密管理性要件の趣旨を、「営業秘密として保護の対象となる情報とそうでない情報とが明確に区別されていなければ、事業者が保有する情報に接した者にとって、当該情報を使用等することが許されるか否かを予測することが困難となり、その結果、情報の自由な利用を阻害することになるからである」とし、前述の「趣旨からすれば、……客観的認識可能性こそが重要であって、」アクセス制限「の点は秘密管理性の有無を判断する上で重要な要素となるものではあるが、②と独立の要件とみるのは相当でない」と判示し、経済産業省の考え方に沿った判断をしたところに大きな意義がある。アクセス制限を独立の要件としないということは、十分なアクセス制限が無いことのみを根拠に秘密管理性が否定されることがないということである。すなわち、アクセス制限がほとんどなされず、杜撰な管理体制であっても、他の要素から客観的認識可能性の要件を満たせば、秘密管理性が認められることにもなりかねない。アクセス制限の要件を客観的認識可能性要件の中に入れ込むことによって、秘密管理性の判断にあたって事案に即した柔軟な判断ができるというメリットはあるが、そもそも、不正競争防止法の目的である「事業者間の公正な競争の確保」に鑑みれば、事業者自体が公正な競争の確保という観点から保護に値するだけの努力をすべき[7]だともいえる。企業の事業活動には不可避的に他社との競争が生じるものであり、他社に出し抜かれないように自己防衛を行うのが原則である。その上で、不公正な競争行為が行われないように法的に保護をするというのが不正競争防止法の趣旨に適うだろう。したがって、十分なアクセス制限や情報管理がなされていないにもかかわらず、被害の大きさや社会的影響を殊更に重視して、安易に秘密管理性を認めること

4）　大阪弁護士会友新会編「最新不正競争関係判例と実務」［第3版］（2016年）52頁。
5）　前掲注3）42頁。
6）　経済産業省「営業秘密管理指針」（2015年）3頁。
7）　田山聡美「刑事裁判例批評（364）」刑事法ジャーナル№56（2018年）　158頁。

は、法の趣旨にはそぐわないと考えるべきである。

もっとも、秘密管理性の認定にアクセス制限を要求するとしても、どの程度までのことを要求するかという問題は残る。経済産業省は、営業秘密管理指針において、「具体的に必要な秘密管理措置の内容・程度は、企業の規模、業態、従業員の職務、情報の性質その他の事情の如何によって異なるものであり、企業における営業秘密の管理単位……における従業員がそれを一般的に、かつ容易に認識できる程度のものである必要がある」[8]としており、明確な基準は示していないが、これは結局のところ、「その情報に接した従業員が、その情報が秘密情報であると認識できる程度の管理で足りる」と言い換えることもできるだろう。民事裁判例においても、そのような緩い管理基準を示したものが存在する[9]。

本件においては、データベースのアカウント情報が社内の共有フォルダ内に蔵置されていて他の従業員でも閲覧可能であったことや本件データベースにアクセスできた従業員の数が特定できなかったことなど、アカウント管理が不十分であったものの、一応はアカウント等によりアクセス制限が行われ、外部記憶媒体への書き出しが制限されており、従業員全員を対象とした情報セキュリティ研修を実施していたという事実もあった。原審においては、これらの事実関係であっても、アクセス制限の要件を満たすと判断したが、本判決は、アクセス制限の不十分さを認めたうえで、一定のアクセス制限の措置がとられていたことを考慮し、秘密管理性を肯定している。果たして、本件において、秘密管理性を認めるだけのアクセス制限措置がなされていたといえるかどうかについては、判断の分かれうるところであり[10]、本判決が、量刑において企業側の情報管理の不備を考慮したということからも、裁判所の悩みが垣間見えるといえるのではないだろうか。

3　営業秘密の管理に係る任務違背

営業秘密の管理に係る任務を負っていなければ、不正競争防止法21条1項3号、4号の罪の主体とならないが、本件では、被告人がBの社員ではなくEの社員であった（BとC、CとD、DとEの間で業務委託契約が結ばれていたが、それらは偽装請負であった）ことから、被告人が、Bに対して営業秘密の管理に係る任務を負うものといえるかが争点となった。

不正競争防止法21条1項3号、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、保有者との委任契約や雇用契約等において一般的に課せられた秘密を保持すべき任務や、秘密保持契約等によって個別的に課せられた秘密を保持すべき任務を意味する[11]。

原審では、BからC、D、Eと順次業務委託契約が締結されており、その各業務委託契約に基づいて被告人が業務に従事しており、各業務委託契約に秘密保持義務の条項があること、業務内容・性質、被告人がEに対して機密情報保持の誓約書を提出していることから、A、Bに対する秘密保持義務を認めた。本判決では、結論としては秘密保持義務を認めたものの、その理由付けが原審と大きく異なる。

本判決は、被告人がEに対して負っていた秘密保持義務の対象には、被告人がBの業務上取り扱っていた機密情報も含まれるものの、このことから当然に被告人が契約当事者としてBに対して秘密保持義務を負うことにはならないとしている。

そして、BとC、CとD、DとEの間の業務委託契約を偽装請負と認定したうえで、被告人がBの指揮命令を受けて業務に従事する者であったことか

8）前掲注6）5頁。
9）「ある情報が秘密として管理されているといえるためには，当該情報がその開示を受けた者等が秘密であると認識しうる程度に管理されていることが必要である」（大阪高判平成20年7月18日　裁判所HP）。
10）本件では秘密管理性は充たされないという見解を論じたものとして、帖佐隆「判例評釈」久留米77号（2017年）206頁。
11）前掲注3）206頁。

ら、労働者派遣法2条2号にいう派遣労働者に当たり、当時はまだ未施行の同法40条の6第1項1号の類推適用により、被告人とB間に直接雇用契約が成立したものとみなし、同法24条の4により、業務上取り扱ったことについて得た秘密を他に漏らしてはならない義務を負うとしている。そして、被告人がBに対して秘密遵守の同意書を提出していたことが、被告人とBとの間の秘密保持契約として有効なものだとして、Bに対する秘密保持義務を認定している。他方で、Aに対する秘密保持義務は認めなかった。

本判決は、被告人とBとの間の直接の秘密保持義務を認めていることから、BとC、CとD、DとEの間の業務委託契約が公序良俗に反し無効であるとしても、被告人の秘密保持義務違反の結論を左右しないという点では、よく組み立てられたものであるといえるが、当時未施行の労働者派遣法40条の6第1項1号を類推適用するという点で、少し技巧的過ぎると言わざるを得ない[12]。原審が、各会社間の業務委託契約に秘密保持義務の条項があることを背景に、被告人とBとの間だけでなく被告人とAとの間の秘密保持義務を認めていることは、少し安易であると考えられるが、本判決のような技巧的な理由付けを用いなくても、少なくとも被告人とBとの間については、被告人がBに対して秘密遵守の同意書を提出していることから秘密保持義務を素直に認める理由付けが有り得たのではないだろうか。

4　量刑

不正競争防止法21条1項違反の罪に対しては、10年以下の懲役もしくは2000万円以下の罰金、又はその併科が規定されている（平成27年改正により罰金が1000万円以下から2000万円以下に引き上げられた。本件に適用されるのは平成27年改正前の同法21条1項。平成27年改正の趣旨は、昨今の情報通信技術の高度化等の社会状況の変化を背景として営業秘密侵害の危険性が高まっていること、近年、大型の営業秘密漏えい事案が顕在化し、営業秘密侵害による損害額も高騰する傾向にあることなどの状況を踏まえ、より実効的な刑事罰による抑止と民事的救済を実現するためということである[13]）。

原審は、被告人を懲役3年6月及び罰金300万円に処し、本判決は、原判決を量刑不当により破棄し、懲役2年6月（実刑）及び罰金300万円に処している。果たして、この量刑は適切といえるだろうか。

不正競争防止法違反の他の著名な刑事事件としては、東芝と提携関係にあったSanDiskの元社員が東芝から技術情報を盗み出し、それを手土産に韓国SK Hynixに役員待遇で転職した東芝データ流出事件において、平成27年9月4日に東京高裁が一審の東京地裁判決を支持し、被告人は、懲役5年、罰金300万円に処されている。東芝データ流出事件においては、民事訴訟において、韓国SK Hynixが東芝に対して約330億円を支払うことで和解が成立している。

本件において流出した情報は、約3000万件にものぼる大量の顧客情報であり、前述のとおり、社会にも大きな影響を与えた事件である。Aは、顧客へのお詫びとして一人あたり500円の金券を配布し、約200億円の損害が生じている。

社会的な影響と損害額だけをみれば、本件と東芝データ流出事件においてそこまで大きな差があるとは考えられない。しかし、東芝データ流出事件においては懲役が5年であるのに対し、本件はその半分の懲役2年6月である。このような差が出たのは、流出した情報が、東芝データ流出事件においては、フラッシュメモリに関する技術情報であるのに対し、本件は、数こそ多いものの顧客に関する氏名、住所、電話番号、性別、生年月日などという単純な

12）本判決の判断に疑問を呈する見解を論じたものとして、前掲注7）159頁、前掲注10）195頁。
13）前掲注3）22頁。

情報に過ぎないという点にあると考えられる。すなわち、企業の商品開発に関する技術情報は、企業の積極的かつ大きな投資や年月を必要とするのに対し、顧客情報は、情報の蓄積に過ぎず、不正競争防止法1条の事業者間の公正な競争の確保という目的に照らせば、顧客情報よりも技術情報の要保護性が高いのである。したがって、不正競争防止法違反の量刑において、東芝データ流出事件と本件を比較した場合に、後者の量刑が前者より軽くなるのは必然である。そして、本件においては、企業側の秘密漏洩対策に不備があったことも、競争原理の中での自己管理原則に照らせば、被害者側の落ち度として、量刑で考慮するのも当然の帰結といえる。そして、本件は、前述のとおり、大規模な情報流出で社会に大きな影響を与えた事件であり、その意味で実刑判決となったことについても首肯できる。結局、本件は、東芝データ流出事件や他の執行猶予が付いた営業秘密侵害事件[14]と比較して、侵害された情報自体の企業活動に対する価値、社会的影響などを考慮すると、適度な量刑であったといえるのではないだろうか[15]。いずれにせよ、不正競争防止法違反（営業秘密侵害）の刑事裁判例は、まだ蓄積が少ない上に、法改正による厳罰化の流れがあることから、今後量刑についても流動的であるといえるだろう。

14）名古屋地判平成26年8月20日、横浜地判平成28年1月29日など。
15）本件が過大な処罰であるとする見解を論じるものとして、前掲注7）160頁、本件は無罪であるとする見解を論じるものとして、前掲注10）185頁。