

営業秘密 平成29年の裁判例 総決算

弁護士知財ネット 関東甲信越地域会
弁護士 岡田 健太郎 (神奈川県)

みなさん平成29年はどんな年でしたか。営業秘密の分野でも、平成29年に新しい裁判例がいくつも出ています。このコラムでは、平成29年に出された営業秘密に関する裁判例をわかりやすくご紹介することで、実際の裁判ではどのような点が問題になっているか、今後の秘密情報の管理に参考にできる点は何か、を検討したいと思います。平成30年がより良い年になるよう、平成29年の裁判例から学んでみましょう。

第1 転職・退職した従業員に絡むケース

東京地裁平成29年10月25日判決

【事件の概要】

転職した元従業員が、転職先の会社において元の会社の顧客情報等を使用して営業活動を行ったとして、転職前の会社が、転職先の会社及び元従業員を訴えた事案。

【判決の結論】

請求棄却。

【事実関係の要点】

元従業員は在職時に秘密保持に関する誓約書に署名押印していた。その誓約書には、「経営上、営業上、技術上の情報の一切」や「原告の顧客、取引先に関する情報の一切」等について、会社在籍中はもとより退職後においても、会社以外の第三者に開示、使用等をしてはならない、と規定されていた。

【判決の要旨1 誓約書の秘密保持条項の有効性】

- ・内容が合理的で、被用者の退職後の行動を過度に制約するものでない限り有効。
- ・不正競争防止法2条6項の「営業秘密」の3要件と同様の要件が必要であり、これを前提とする限りにおいて、本件秘密保持条項は有効。

【判決の要旨2 秘密管理性】

結論：秘密として管理されていなかった。

理由： ①規格書等は、原告の役員及び従業員の各自のコンピュータからアクセス可能なサーバに保管されており、原告従業員が閲覧、印刷、複製できる状態にあった。

②原告は、得意先・粗利管理表が、原告代表者のパソコン内に入れられてお

り、他の従業員はアクセスできない状態にあったと主張するが、被告は、従業員のパソコンからもアクセスすることができたと供述しており、従業員全てがアクセスできないような形で保管されていたことを客観的に示す証拠はない。

③原告は、得意先・粗利管理表を、「社外持出し禁」と表示した書面とともに配布していたと主張するが、それを客観的に示す証拠がない。

なお、本判決では、被告が原告の秘密情報を使用したという点も、「認めることができない」として、否定された。

【学ぶべきポイント】

平成27年に全部改訂された経済産業省の営業秘密管理指針では、「秘密管理性要件が満たされるためには、営業秘密保有企業の秘密管理意思が秘密管理措置によって従業員等に対して明確に示され、当該秘密管理意思に対する従業員等の認識可能性が確保される必要がある。」とされています。

本件判決は、原告が小規模な会社であることを考慮しても、原告の情報の管理状況によれば、その従業員が秘密と明確に認識し得る形で管理されていたということではできず、秘密として管理されていたということではできない、と判断しています。

秘密管理措置を取ることによって、従業員に明確に示すようにしていれば、いざ裁判になったときにも、秘密管理措置の内容を証拠として提出することが容易になってきます。例えば、秘密情報が記載された印刷物それ自体に「社外秘」などの記載をしておけば、その印刷物自体を証拠として提出することができます。今回の原告が主張したように、「社外持出し禁」と表示した書面とともに、情報の記載した書面を配布していたというのでは、本当に一緒に配布していたのか、という疑問がどうしても出てきます。

従業員に明確に分かる形で秘密管理措置を取るということは、後に裁判になったときにも、証拠として提出しやすく、立証が容易になるということにもつながります。

大阪地方裁判所平成29年10月19日判決

【事案の概要】

会社の開発課に所属し、技術情報にアクセスする権限を有していた従業員（その後懲戒解雇）が、在職中に競合他社への転職を視野に入れ、技術情報の電子データを、会社から支給されたものではないUSBメモリに複製した。会社（原告）が当該元従業員（被告）に対し、不正の利益を得る目的で、競合他社に開示し、あるいは使用するおそれがあるとして、不正競争防止法2条1項7号に基づき、使用及び開示の差止請求等をした。

【判決の結論】

- ・使用及び開示の差止め、電子データ及びその複製物の廃棄、損害賠償は、認容。
- ・電子データ及び複製物の返還請求は棄却。

【情報の管理状況】

本件の技術情報は、Yドライブ（社内LANに接続せずにスタンドアロン状態で使用され、被告を含む開発課の従業員（4名）が共有のサーバとして利用するために設置された市販されている小型のネットワークHDD）に電子データとして保存されていた。その後、Yドライブを社内LANに接続することになり、その際、開発課の従業員4名のパソコン1台1台にYドライブに接続するのに必要なプライベートIPアドレスを設定してアクセス制限を施した。

【秘密管理性についての判示】

本件電子データを含むYドライブに保存された電子データは全て原告によって秘密として管理していたと認められる。

【被告が技術情報を複製した際の状況】

被告は休日に業務命令によらず出勤し、技術情報のデータを原告の支給品ではない外付けHDDに保存した。被告はその作業中、業務用端末PCからLANケーブル抜いている。また、同僚が出勤した後間もなくパソコンの作業を止めて帰宅した。また、被告は、後日、あえて時間と手間がかかり電子データの復元が困難となる方法で被告業務用外付けHDDからデータの消去作業を行った。

【学ぶべきポイント】

本件の技術情報は、国内及び海外でも同業が数社しかいないというような技術に関する情報であり、管理体制もある程度しっかりできていたことから、不正競争防止法に基づく差止請求ができたと考えられます。

社内ネットワークを構築する際には、秘密情報についてはアクセスできる従業員を限定することで、秘密管理性が認められやすくなります。

いったん情報の流出が疑われた場合には、ログなどの痕跡をきちんと保全しておくことの重要性もこの裁判例から学ぶことができます。

控訴審：大阪高等裁判所平成29年7月20日判決

原審：大阪地方裁判所平成29年1月12日判決

【事案の概要】

介護サービス事業を営む会社（原告）に、ケアマネージャーとして勤務していたAが、会社を退職し、介護サービス事業を営む新しい会社を設立した。

本件は、原告が、Aや他に退職したケアマネージャー、訪問介護事業のサービス提供責任者などを被告として、これらの者が原告の営業秘密である利用者の情報を持ち出し、不正の利益を得る目的、あるいは、原告に損害を加える目的で、同情報を使用して原告の利用者を勧誘するなどしたとして差止及び損害賠償を請求した事案。

【判決の結論】

大阪地裁は、被告らに不正競争は認められないとして請求を棄却し、大阪高裁も基

本的に同じ理由で控訴を棄却した。

【情報の管理状況】

介護サービス利用者の氏名、年齢、電話番号、介護認定状況等の情報（利用者情報）が記載された利用者名簿が、紙媒体の一つのファイルとして、施錠できるキャビネットに保管されていた。原告事業所に人がいない場合にはキャビネットは施錠されることとなっており、鍵はキャビネットの裏に置かれていた。

また、利用者情報は、電磁的記録として、クラウドコンピューティングシステムである「楽にネット」に保存され、被告3名を含む4名の従業員各自にセキュリティーキーが配布され、セキュリティーキーにID、パスワードが設定されていた。

被告らの雇用契約書には、業務上知り得た利用者又はその家族の秘密を保持しなければならないと定められている。

【秘密管理性についての判決内容】

利用者情報は、利用者のプライバシーに係る情報を含むものであり、従業員において秘密保持の対象となるものである。

利用者情報は、キャビネットに保管することが予定されていたものである。

被告A自身も、介護事業者としての指定を受ける際に、キャビネットに施錠して保管するよう求められていることを認めている。

このような利用者情報の管理状況からすれば、利用者情報は、原告事務所に勤務する原告従業員のみが利用できるもので、他に漏らしてはならない営業上の情報であると認識できたものといえ、秘密として管理されていたものである。

【被告らの不正競争の有無】

被告Aが有給休暇中に利用者情報にアクセス可能となるセキュリティーキーを自宅に持ち帰って2度ほどアクセスし、また休暇中に2度ほど原告事務所に出社している。しかし、ケアマネージャーとして必要な書類につき未処理のものの作成等を行う必要があったといえ、利用者情報を不正に取得したと推認することはできない。

原告から被告会社に移った利用者も相当程度いるが、原告が居宅介護支援事業を取りやめたとか、ケアマネージャーの移籍に伴い、利用者も被告会社に移ったにすぎない。

原告の就業規則や被告らの雇用契約に、退職後の競業避止義務を定めた規定は見当たらない。

したがって、被告らには不正競争は認められない。

【学ぶべき点】

経済産業省の営業秘密管理指針では、「個々の文書やファイルに秘密表示をする代わりに、施錠可能なキャビネット等に保管する方法も、認識可能性を確保する手段として考えられる。」（同9頁）とされています。ただ、実際は、キャビネットに施錠する方法よりも、「社外持出し禁止」や「社外秘」などの表示をする方が、手軽で業務への

支障が少ないように思われます。

また、本件では、秘密管理性は肯定されたものの、不正使用が認定できないと判断されています。本件では、職務上、秘密情報にアクセスする必要性があり、アクセスしていたとしても不自然ではないという事例であり、ケアマネージャーという利用者との個人的なつながりが重要視される事案であったことも結論に影響しているのではないかと考えられます。なお、一般的には、不正使用を後に立証できるようにするために、使用の記録が残るような措置を講じておくことが有用です。

第2 業務提携した会社間における事案

知的財産高等裁判所平成29年2月23日判決

【事案の概要】

控訴人（原告）は、被控訴人（被告）との間で、被控訴人が控訴人に対して事業に関するコンサルタントを行い、控訴人が被控訴人にノウハウの提供等を行うという業務委託契約を締結していた。

控訴人は、被控訴人による本件文書1～3の持ち出し及び使用行為が、債務不履行（「相手から入手した秘密情報」の目的外使用）又は不正競争に当たるとして、被控訴人に対し損害賠償等を請求した。

【不正競争についての判決の要旨】

控訴人代表者が本件の試薬の開発に当たって中心的な役割を果たしたものと推認されるが、控訴人と被控訴人の間では、試薬について開発委託契約又は共同研究開発契約は締結されておらず、試薬の開発に伴う知的財産権やノウハウの帰属に関する明示的な合意は見当たらず、かえって業務委託契約等では産業財産権の帰属は共有とすると規定されていた。

したがって、本件秘密情報を含む知的財産権やノウハウが、控訴人のみに帰属し、控訴人の営業秘密として、被控訴人がこれを使用することができないものであるとは言えない。

そうすると、被控訴人が本件秘密情報を持ち出した行為が仮に認められるとしても、不正競争防止法2条1項4号～6号所定の不正取得行為に当たらないから、不正競争には当たらない。

東京地方裁判所平成29年2月9日判決

【事案の概要】

原告と被告A社は、継続的な靴の製造委託契約を締結し、被告A社が靴の製造を行い、原告から委託報酬を受けていた。被告A社は、原告が企画開発する靴のオリジナル木型（木型製作会社Cが製造し保管するマスター木型に基づいて作成される木型）

を預かっていた。

原告は、被告A社がオリジナル木型を被告B社らに不正に開示する等の行為をしたとして、不正競争防止法2条1項7号の不正競争であると主張して、被告らに対し差止めや損害賠償を求めた。

【秘密管理性について】

①原告においては、従業員から原告に関する一切の機密を漏えいしない旨の誓約書を徴するとともに、就業規則で目的外使用や職務外使用を禁止していたこと、②業界においてマスター木型やオリジナル木型が生命線ともいうべき重要な価値を有することが認識されており、マスター木型は木型製造会社Cで厳重に管理されていたこと、③原告においては、通常、マスター木型やオリジナル木型について従業員が取り扱えないようにされていたことが認められる。これらからすると、原告の従業員は原告の秘密情報であると認識していたものであり、取引先製造受託業者もその旨認識し得たものであり、秘密として管理されていたといえる。

⇒原告の請求は認容された。

第3 第三者（知財紛争の相手方）の不正取得が争われた事案

東京地方裁判所平成29年7月12日判決

【事案の概要】

A社は、B社の製造販売する製品がA社の特許権を侵害するとして、特許権侵害訴訟の提起と仮処分の申立てを行い（別件訴訟等）、B社製品の動作、構造等を特定する証拠又は疎明資料として、B社製品の製品概要、仕様等が記載され、各丁に「CONFIDENTIAL」との記載がある文書等を裁判所に提出した。

これに対し、B社は、A社が不正開示行為が介在したことを重大な過失により知らないで当該文書を取得し、使用したとして、A社の行為が不正競争防止法2条1項8号に該当すると主張し、A社を被告として訴訟を提起した（本件訴訟）。

【判決の要旨】

本件の文書は、B社が中国企業に対してB社製品を販売する目的で台湾の代理店や中国企業に提供したものであり、その内容も、A社が自社の製品に取り入れるなどした場合にB社に深刻な不利益を生じさせるようなものではない。

A社がその営業活動の中でB社が営業している製品の情報を得ることは当然に考えられ、その一環としてB社製品の製品概要、仕様等が記載された本件文書を取得することは不自然とは言えない。

したがって、仮に不正取得行為が介在していたとしても、A社が不正開示行為が介在したことを重大な過失により知らないで本件の文書を取得したと認めることはできない。

【学ぶべき点】

「CONFIDENTIAL」等、秘密情報であることが客観的に分かる表示をすることは営業秘密として保護されるために重要です。ただ、本件では、そのような印字があったとしても、文書の内容や性質等から、営業秘密としての保護に値する情報であるかどうかについて、疑問があったと考えられます。しかも、本件では、不正取得行為が具体的に特定できないという事案であり、上記のような文書の内容等も併せて考えると、不正取得が介在していたことを重大な過失により知らないで文書を取得したということを認定するのは困難な事例であったと考えられます。

第4 会社資産の売却に伴う営業秘密流出が争われた事例

東京地方裁判所平成29年1月26日判決

【事案の概要】

原告は、学習教室の経営等を行う会社である。原告の代表取締役である被告Aが、原告の様々な資産と共に、顧客情報が入ったパソコンを被告B社に対して売却した（その後、Aは退任）。原告は、一連の財産処分行為が被告Aの取締役としての任務懈怠行為に当たると主張して会社法に基づく損害賠償を請求すると共に、被告B社らが顧客名簿を不正使用していると主張して、不正競争防止法2条1項7号に基づく損害賠償を請求した。

【顧客名簿の管理状況】

①原告は新たな顧客を獲得した場合、顧客の名称又は氏名及び住所等が記載された注文書をファイルに綴って取引先を整理していた。

②次いで、原告は、一覧性を高めるために、注文書等を基にして、一覧表を作成していた。注文書等を綴ったファイル、紙媒体の一覧表は、原告の従業員及び講師であればいつでも見ることができた。

③原告は、①、②に加えてさらに詳細な情報をパソコンに入力して顧客名簿を作成していた。このパソコンを起動するためにはパスワードが必要であったが、本件の顧客名簿のデータにはパスワードの設定はなかった。

【営業秘密該当性の判断】

①注文書等を綴ったファイル、②紙媒体の一覧表については、閲覧や利用が制限されていなかったと認められる。

また、③パソコン内の顧客名簿についても、パスワードの管理状況やアクセスし得る者の範囲を的確に認定するに足りる証拠はない。

そうすると、本件の顧客名簿に含まれる情報が秘密として管理されていたということとはできず、不正競争防止法2条6項の営業秘密に当たるとは認められない。

【コメント】

本件は、一連の財産処分行為の違法性がメインの論点になっており、被告Aらに対する損害賠償責任が認められています。したがって、営業秘密性を否定したとしても、原告側に重大な影響が生じない事案であったと言えます。

第5 慰謝料が問題となった最高裁判決

最高裁判所平成29年10月23日第二小法廷判決

【事案の概要】

本件は、上告人が、被上告人において管理していた上告人の個人情報を通じたことにより精神的苦痛を被ったと主張して、被上告人に対し、不法行為に基づき、慰謝料及び遅延損害金の支払を求める事案である。

上告人は、未成年者であるBの保護者であり、被上告人は、通信教育等を目的とする会社である。被上告人が管理していたBの氏名、性別、生年月日、郵便番号、住所及び電話番号並びにBの保護者としての上告人の氏名といった上告人に係る個人情報（本件個人情報）が、外部に漏えいした。

本件の漏えいは、被上告人のシステムの開発、運用を行っていた会社の業務委託先の従業員であった者が、被上告人のデータベースから被上告人の顧客等に係る大量の個人情報を不正に持ち出したことによって生じたものであり、上記の者は、持ち出したこれらの個人情報の全部又は一部を複数の名簿業者に売却した。

【原審の判断】

本件漏えいによって、上告人が迷惑行為を受けているとか、財産的な損害を被ったなど、不快感や不安を超える損害を被ったことについての主張、立証がされていないから、上告人の主張は、その余の点について判断するまでもなく理由がない。

【最高裁の判断】

破棄差し戻し。

本件個人情報は、上告人のプライバシーに係る情報として法的保護の対象となるというべきであるところ、本件の事実関係によれば、本件漏えいによって、上告人は、そのプライバシーを侵害されたといえる。

しかるに、原審は、上記のプライバシーの侵害による上告人の精神的損害の有無及びその程度等について十分に審理することなく、不快感等を超える損害の発生についての主張、立証がされていないということのみから直ちに上告人の請求を棄却したものである。原審の判断には、不法行為における損害に関する法令の解釈適用を誤った結果、上記の点について審理を尽くさなかった違法がある。

第6 刑事事件

福岡地方裁判所平成29年10月16日判決

【公訴事実の概要】

被告人は、株式会社A銀行から、同社において秘密として管理している事業活動に有用な顧客の氏名及び住所等の情報であって、公然と知られていないもの（顧客情報）を、閲覧する権限を付与され、営業秘密を同社から示されていた者であるが、顧客情報の照会オペレーションは、業務上必要なものに限り、かつ、顧客情報については、みだりにコピーをとってはならない旨の営業秘密の管理に係る任務に背いて、同社のサーバコンピュータにアクセスして、営業支援システムを起動させ、預金額が1億円以上の同社の顧客らを検索するなどし、同顧客らの氏名及び住所等の検索結果を紙面に印字するなどの方法により領得した顧客情報が記載された顧客名簿を、不正の利益を得る目的で、顧客情報を第三者に開示してはならない旨の営業秘密の管理に係る任務に背き、Cに交付し、もって営業秘密を開示した。

【コメント】

公訴事実の記載内容からすると、不正競争防止法21条1項4号の構成要件に該当すると判断されていると考えられます。

本件の被告人は、他の共犯者と共謀の上、金品窃取の目的で銀行の支店に侵入し、現金を窃取したという、建造物侵入、窃盗の罪なども犯しており、それらも合わせて懲役6年という重い判決となっています。

本件で適用されている通り、不正競争防止法には刑事罰が規定されています。平成27年の改正では、同法21条1項の罰金の上限が1000万円から2000万円に引き上げられるなど、厳罰化の方向での改正が行われています。

東京高等裁判所平成29年3月21日判決

【事案の概要】

被告人は、通信教育等を業とするA社がB社に業務委託したA社の情報システムの開発等の業務に従事し、営業秘密であるAの顧客情報を、これが記録されたA社のサーバコンピュータに業務用PC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示されていた。被告人は、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合計約2989万件の顧客情報データをダウンロードして業務用PCに保存した上、自己のスマートフォンの内臓メモリ又はマイクロSDカードにこれを記録させて複製する方法により、上記顧客情報を領得し、②そのうち約1009万件の顧客情報について、名簿業者に開示した、という事実により、不正競争防止法違反に問われた。

【判決の内容】

第1審：懲役3年6月及び罰金300万円

第2審：懲役2年6月及び罰金300万円

【秘密管理性についての判断基準】

原判決は、秘密管理性の要件について、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、という2つの要件を提示していた。

これに対し、控訴審判決は、②の客観的認識可能性こそが重要であって、①のアクセス制限は、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、と判示した。

その上で、控訴審判決は、所論がいうように、A社が、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、と判示した。

【秘密管理性についてのあてはめ】

毎年、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、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等のほか、個人情報及び秘密情報の秘保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社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。

⇒秘密管理性を肯定。

【学ぶべきこと】

平成27年1月28日に全部改訂された経済産業省の営業秘密管理指針は、「秘密管理性要件が満たされるためには、営業秘密保有企業の秘密管理意思が秘密管理措置によって従業員等に対して明確に示され、当該秘密管理意思に対する従業員等の認識可能性が確保される必要がある。」とされ、「アクセス制限」は「認識可能性」と別個の要件ではなく、「認識可能性」を担保する一つの手段であると考えられる、と整理されています。

本件の控訴審の判決は、この営業秘密管理指針の考え方と同様の考え方を示すものであると言えます。