連邦営業秘密防衛法（DTSA）をめぐる実務上の諸問題

―Waymo v. Uber 事件の教訓およびDTSAが実務にもたらす影響を中心として―

James POOLEY, Mindy M. MORTON, 山根　崇邦
山根　崇邦（訳）

はじめに

本稿は、2018年５月22日に米国のProcopio法律事務所（カリフォルニア州パロアルト）で開催された第９回ベイエリア知財セミナー（Bay Area CHIZAI (IP)）のパネルディスカッションの記録を翻訳したものである。パネルディスカッションの録音データの文字起こしにあたっては、NEDOシリコンバレー事務所の泉卓也氏と橋本こず恵氏のご尽力を得た。記して感謝申し上げる。

ベイエリア知財セミナーは、泉卓也氏（NEDOシリコンバレー事務所次長）と竹中俊子教授（ワシントン大学・慶應義塾大学）が2016年11月に立

ち上げた研究会である。本セミナーは１～２ヵ月に一度の頻度で開催され、毎回、講師による講演（時折パネルディスカッション）、フリーディスカッション、ネットワーキングの形式で行われている。本セミナーには、ベイエリアで活躍する現地の弁護士やパテントエージェント（インハウスを含む）、日系企業の駐在員、スタンフォードやバークレーなどベイエリアのロースクールに留学中の日本人などが多数参加しており、ベイエリアにおける日米知財関係者の交流の場として注目を集めている。

第９回セミナーは、２部構成で行われた。第１部では、筆者（山根）が講師を務めた。カリフォルニア大学バークレー校ロースクールにおける在外研究の成果報告を兼ねて、2016年５月11日に成立した連邦営業秘密防衛法（Defend Trade Secrets Act of 2016: DTSA）の現状について報告を行った。報告では、DTSA施行後の１年間の裁判例の動向をもとに、日本の営業秘密訴訟と比較しながら、営業秘密保護の実態について議論した。この報告内容をまとめたものが、本号から掲載される拙稿「アメリカにおける営業秘密の保護－連邦営業秘密防衛法（DTSA）の運用実態と日本の営業秘密訴訟との比較」である。

一方、第２部では、DTSAをめぐる実務上の諸問題についてパネルディスカッションを行った。パネリストは、米国営業秘密法の第一人者であり、DTSAの制定過程および制定後の二度にわたって上院・下院司法委員会の公聴会で専門家証言を行ったJames Pooley弁護士[1]、Procopio法律事務所の

[1] 1948年米国オハイオ州生まれ。1970年にラファイエット・カレッジを卒業（B.A. with honors）、1973年にコロンビア大学ロースクールを修了（J.D.）。35年以上にわたって知財訴訟（中でも営業秘密・特許訴訟）を専門とする弁護士として活躍した後、ホワイトハウスからの任命によりWIPO事務局次長に就任（2009-2014年）。2015年に弁護士として復帰。この間、カリフォルニア大学バークレー校ロースクール非常勤教授を兼任（営業秘密法担当、1998-2009年、2017年-）。専門的な体系書としてTRADE SECRETS (Law Journal Press, 1997-updated semiannually)、論文としてJames Pooley, *The Myth of the Trade Secret Troll: Why the Defend Trade Secrets Act Improves the Protection of Commercial Information*, 23 GEO. MASON L. REV. 1045 (2016); James H.A. Pooley, Mark A. Lemley & Peter J. Toren, *Understanding the Economic Espionage Act of 1996*, 5 TEX. INT. PROP. L.J. 177 (1997)、一般書としてSECRETS: MANAGING INFORMATION ASSETS IN THE AGE OF CYBERESPIONAGE (Verus Press, 2015); TRADE SECRETS: A

パートナーであり、ベイエリアにおいて営業秘密をはじめとする知財訴訟で活躍するMindy M. Morton弁護士[2]、筆者の3名が務めた。Morton弁護士には司会もお願いした。ご多忙の中、パネリストおよび司会をご快諾いただいたPooley弁護士、Morton弁護士には、この場を借りて改めて御礼を申し上げたい。

パネルディスカッションでは、①Waymo v. Uber事件の教訓、②DTSAの成立によって営業秘密の風景は変わるか？、③オープンイノベーションと営業秘密、④秘密保持のための合理的措置に関する日米比較という、4つのテーマについて議論した。事前に主催者側から企業実務にとって参考になる点を中心にディスカッションをお願いできればという要望があったため、当日は実務経験が豊富なPooley弁護士とMorton弁護士に議論をリードしていただき、適宜私から質問やコメントをしたり、フロアから質問を受けたりする形で、パネルディスカッションが進められた。

以下、パネルディスカッションの記録を掲載する。わが国の今後の営業秘密法制を考えるうえで、少しでも参考になるところがあれば望外の喜びである。(文責：山根)

1．Waymo v. Uber事件の教訓

Morton： 今日は、4つのテーマについて議論したいと思います。それぞれのテーマについて話し合った後で、質疑応答を予定しています。最初のテーマは、Waymo v. Uber事件[3]です。この事件について、まずPooley弁

GUIDE TO PROTECTING PROPRIETARY BUSINESS INFORMATION (AMACOM, 1987)［鳥井厚夫＝大橋正春訳『営業秘密管理の手引き』(中経出版、1991年)］等がある。

[2] 1994年にカリフォルニア大学バークレー校を卒業(B.A. with highest honors)、1997年にイエール大学ロースクールを修了(J.D., Yale Law Journal編集委員)。知財訴訟の中でも、営業秘密、インターネット法、特許、商標、著作権、コンピュータ犯罪、競業避止契約の訴訟を専門とする。

[3] 本件訴訟は、2017年2月23日に提起され、2018年2月9日に和解により終結した。本件では多数の命令や意見が出されているが、主要なものとして、Waymo LLC v. Uber Techs., Inc., 2017 U.S. Dist. LEXIS 73843 (N.D. Cal. May 11, 2017); Waymo LLC v. Uber Techs., Inc., 2017 U.S. Dist. LEXIS 183688 (N.D. Cal. Nov. 2, 2017); Waymo LLC v.

護士に話してもらいます。

(1) 事件の概要と教訓

Pooley： この事件が今回の議論のテーマとしてふさわしいのは、提訴からまだ1年弱しか経っていない段階で結審したからです。つまりこれは、連邦裁判所ではこの種の事件の審理に時間がかからないことの証と言えます。その理由は、州裁判所よりも連邦裁判所の裁判官の方が、裁判の日程について大きな権限を持っているからです。ですから、規模が大きい事件、つまり当事者が複数の州や国にまたがる事件が連邦裁判所に持ち込まれるのも、当然の話なのです。連邦裁判所の裁判官は時間をかけて入念に審理してくれますから。ただし、Waymo事件の教訓としては、まさに連邦裁判所であったがゆえに、当事者が期待する以上の権限を持って、裁判官が裁判を差配できたということがあります。当初、担当の裁判官（Alsup判事）は、Waymo社が勝訴するだろうと考えていました。彼も言っていましたが、この事件では、これまで聞いたこともないような極端な事実が明らかになっていましたから。ところが数ヵ月後には、裁判官はWaymo社にこう伝えたのです。今回、あなた方が起こした訴訟はどっちに転ぶかわからない、勝訴するだろうとは到底言えない、ディスカバリーをもう少しだけ続けさせてあげるが、だからと言って、どうなるものでもないだろう、と。そして彼は、まるで特許のクレームのように、営業秘密の対象をきわめて詳細に特定するようにWaymo社に命じました。これは、Waymo社にとって、他の裁判所で裁判を起こす場合よりも営業秘密に係る請求の範囲を狭くせざるを得ないことを意味したのです。

このように、Waymo事件の裁判から明らかなのは、裁判官に十分な時間的余裕がある連邦裁判所で裁判を闘うことの効果です。一般論として、連邦裁判所に訴訟を提起するのはいいことです。ただし、裁判官がその事例について詳細に検討し、その事例をどのようにして棄却しようかと考えている場合には、連邦裁判所で争うことが必ずしもいいことづくめではない

Uber Techs., Inc., 2018 U.S. Dist. LEXIS 8263 (N.D. Cal. Jan. 18, 2018); Waymo LLC v. Uber Techs., Inc., 2018 U.S. Dist. LEXIS 10823 (N.D. Cal. Jan. 18, 2018); Waymo LLC v. Uber Techs., Inc., 2018 U.S. Dist. LEXIS 16020 (N.D. Cal. Jan. 29, 2018)。

ことがわかります。今回の事例では、当初、注目を浴びて、どのような結末になるかとびくびくしていたのはUber社の方でした。暫定的差止命令（preliminary injunction）が認められた時点で、すでにLevandowskiは解雇されていたうえに、修正第5条に基づいて証言を拒否する権利を行使していましたから。しかも担当の裁判官は、自らが下す差止命令を確たるものにするために、刑法上の不正利用の捜査を当局に委ねました。

ではなぜ、最終的にこの事件は、それほど高額ではない和解金の支払いで決着したのでしょうか？つまり、Waymo社は20億ドル近い損害賠償を請求していたにもかかわらず、なぜ2億4,500万ドル相当のUber株の譲渡で和解したのでしょうか？

１つの理由として、担当の裁判官が、Waymo社側が採用した損害額評価の専門家（damages experts）の証言を排除したことが挙げられます。この点についても、やはり連邦裁判所の裁判官の方が、州裁判所の裁判官よりも、担当する事件に対してはるかに懐疑的なのです。この結果、今回の事件でWaymo社は、自身が採用した重要な専門家証人の一人に証言させることができなくなりました。

もう１つ、訴訟の中でさらなる証拠が明らかになったことで、裁判所の認識が変化したことが挙げられます。当初この裁判は、Waymo社にきわめて有利だと思われていました。なにせLevandowskiは、14,000件もの機密ファイルをダウンロードし、その行為を隠蔽しようとして捕まるという、きわめて悪質な行為を行ったのですから。明らかになった事実は、許しがたいものばかりに思われました。しかもUber社は、Levandowskiを採用し彼の会社を買収する前に調査を行い、その調査の結果、彼がかなり悪質な行為を行い、嘘をついている可能性があることを知っていました。にもかかわらずUber社は、買収を断行したのです。それだけではありません。同社はLevandowskiとの間で、Waymo社在職中の彼の行為について、彼の退職後にWaymo社が行う請求から彼を免責するという内容の契約を結んだのです。企業が、競合他社から引き抜いた人物の免責を認めるなんて異例のことです。それ以上に異例だったのは、Uber社が、同社に転職した後のLevandowskiの行為を根拠にWaymo社が不正利用の請求を行った場合、彼の行為が、彼がWaymo社在職中から記憶していた情報に基づいている場合については、Waymo社の請求から彼を免責すると約束したことです。

しかも、このような免責を認めることで、Uber社はきわめて大きなリスクに晒されることになったのです。

しかし、Uber社は努力の甲斐あって、14,000件のファイルのいずれも同社に渡っていないことの証明に成功しました。しかも暫定的差止命令の審尋で、裁判官は、同社の証明の信憑性をかなり高く評価したのです。ただし裁判官は、Uber社にこう尋ねました。「ところで、おそらくLevandowskiは、最後の８～９ヵ月の間、毎晩自宅で14,000件のファイルを読んだ翌日、会社に出勤すると、技術者にいろいろな指示を出していたのでしょうね。そうした指示は、彼がWaymo社から持ち出した情報に基づくものなのですか？」これは、Uber社にとって答えづらい、というか事実上、自分たちの主張を否定することに繋がる質問でした。Levandowskiが修正第５条に基づいて黙秘権を行使したために、Uber社は彼を証人として召喚することができなかったのですから、なおさらです。

しかし、結局のところ、Uber社は幸運だったと言えます。技術開発で、Waymo社が採用していた技術とは別の技術を採用するという決断を下していたのですから。そのおかげで、こう主張できたのです。「Levandowskiがどんな情報を記憶していたのかは知りませんが、わが社ではそれを採用することができませんでした。そもそもわが社はそれを入手しなかったのですから。わが社が入手したという証拠は何一つありません。それにわが社ではWaymo社とは違う技術を採用していたのですから、彼がわが社に情報を教えようとしたところで、そんなことにわが社が興味を持つはずはありません。」これこそ、今回の事件が、途中で失速してしまったというか、尻切れとんぼに終わった原因だと思います。もちろん、トライアルでは、Uber社のTravis Kalanick元社長兼CEOが証人として登場し、大方の予想を裏切って、証人としての役割を見事に果たしたということもありました。その後、経営陣全員が登場し、少なくとも同じ年にカリフォルニア州北部地区で行われたトライアルの中で最も大々的に報道されたトライアルとなりましたが、その４日目の審理が終わった段階で、突然、両当事者は和解したのです。

これは、こうした類の裁判で双方の当事者が大きなリスクを負うことを示す典型的な例でしょうね。営業秘密をめぐる訴訟で重要な要素は、悪しき行為の態様に関係があります。今回は、この要素のおかげで、裁判が前

に進んだのです。明らかと思われたのは、Levandowskiの行為がきわめて悪質なものだったことです。Uber社はきわめて大きなリスクを負っていました。今回の事例は裁判で決着を付けるべきもののように見えましたが、裁判が続くことで、深刻なリスクに晒されることも数多くありました。結局最後に、Waymo社は悟ったのだと思います。この裁判で20億ドルの損害賠償を勝ち取ることはできないだろう、自分たちの思い通りに裁判は進まないだろうと。そこで、裁判での決着を断念したのです。山根先生も同じご意見だと思いますが、今回の事件は、この種の裁判に関心を持つ私たちにとって、まるでドラマのような争いが劇的に展開する様子を目の当たりにできたという意味で、きわめて貴重な経験でした。

(2) その他の実務上の論点

Morton： ありがとうございました。今回の事件については、2、3お聞きしたいことがあります。今回はトライアルまで行ったわけですが、米国では、営業秘密をめぐる事件がトライアルまで行くことはよくあることなのですか?

Pooley： その点に関して言うと、営業秘密のケースは、他の多くのケースと似ています。ビジネス訴訟の場合、トライアルに至らず和解で決着する確率は90%を超えています。営業秘密をめぐる事件に関しては、暫定的差止命令が下された時点で、当事者は、自分たちのリスクが今後どうなるのかを知り、なんとかして和解に持ち込もうとするケースが多いのです。そうした状況では和解が最良の選択肢ですから。その一方で、こうした事件が感情に左右されやすい点は、すでに誰もが知るところです。そのため、無駄に裁判を長期化させるという決断を経営陣が下す場合もあるのです。ただし、結局彼らも莫大な費用とリスクに嫌気が差してしまいます。90%以上の事件は和解で解決するのですから。もちろん、時々はWaymo事件のように、かなり裁判が進んでから和解で決着する場合もありますが。

フロア： こうした事例でいつも頭を悩ませるのが、どこで線引きをするかということです。つまり、会社の所有物と個人の所有物をどこで区別すればいいのかということですね。たとえば今回の場合、Levandowskiは私用のコンピュータを持っており、一部では、問題のファイルがこれに保存されていたと考えられていました。彼が私物を会社に持って行ったりし

ていたかどうかはわかりませんが、従業員が私物を会社に持ち込み、業務で使用することに関する社内方（Bring Your Own Device policy）では、それほど明確な区別がなされていない場合もあります。皆さんは、裁判所がどのような線引きをしているとお考えですか？企業が従業員を雇用する際に、従業員ですら会社の所有物ではないとわかるものを、絶対に社内に持ち込ませないための最善の方法とは、どのようなものなのでしょう？

Pooley：　いい質問ですね。従業員が使う機器の所有権はどのような効果を持っているのでしょうか？数年前に、私物の機器の社内への持ち込みを禁止しようした企業が敗訴したのは有名な話です。しかも今や、従業員が職場に私物の機器を持ち込み、会社のネットワークに接続して使用するなんてことは、ごく当たり前に行われています。スマートフォンやタブレットといった機器を職場では会社のネットワークに接続し、夜、自宅に戻ってからは、その機器を使って、世界中の人たちと自分たちの生活に関するすべての情報を共有するという、ソーシャルメディアでは普通のことをするのです。そして翌日には再びその機器を会社に持って行き、会社のネットワークに接続して、仕事に必要な情報にアクセスするのです。実際に明らかになる問題は、その機器が誰のものなのかということにはほとんど関係がありません。問題は、アクセス可能な情報で従業員が何をしたかということなのであって、場合によっては、アクセスが禁止されている情報にアクセスするために、越えてはいけない一線を越えたのかどうかということが問題になるのです。要は情報が重要なのです。Levandowskiの場合、退職の１ヵ月前に、問題となっているファイルをすべてダウンロードしたうえで、それを複数のCDに移しました。そしてその後、どうやら彼はそのCDを廃棄したらしいというか、廃棄したと主張しています。彼が自らのラップトップ・コンピュータという媒体を使って行ったのが、こうした行為だったのです。ここでは、その機器の所有者が誰かという点は問題ではありませんでした。

Morton：　２、３点付け加えさせてください。まず、最近、私が最大の問題だと感じていることの１つに、フラッシュ・ドライブがあります。皆さん、持っておられますよね。私もいくつかカバンに入れて持ち歩いています。最近、多くの会社では、従業員に対し、私物のフラッシュ・ドライブを会社のコンピュータやネットワークに接続することを禁じています。だ

からと言って、情報のダウンロードが防げるわけではありません。ダウンロードの方法ならほかにもありますから。従業員が新しい方法を見付けると、企業側がその対応策を探すという、一種のいたちごっこが続いています。ただし、特に最も重要な情報に関しては、企業は技術上、さまざまな制限を課すことができます。

もう1つ付け加えさせてもらいたいのは、所有権についてはPooley弁護士と同意見だということです。ほとんどの企業は従業員と契約を結んでいて、それによれば、私物の機器を使用しても構わないけれど、その機器に保存されたいずれの会社の情報も、会社に属するとされています。これに関して興味深いのは「ノウハウ」です。Levandowskiは何を記憶していたのでしょう？これは、まさにWaymo事件で問題になった点です。カリフォルニアでは、従業員が、その分野の一般的な知識を転職の際に持ち出すことが許されています。それが認められなければ、今のようなシリコンバレーは存在していないでしょう。ただし、専門的なノウハウについては、それを転職先の企業で使用することはできません。今回の事例でわかるように、これについては一般的知識とは全く別の扱いになるのです。

Pooley： その点については、これまでもいろいろ議論されています。その理由の1つとして、Morton弁護士が指摘したようなノウハウが、こうした状況では、いわゆる「ネガティブ」インフォメーションに係る営業秘密だという点があります。ネガティブ・インフォメーションに係る営業秘密というのは、望ましい成果を達成しないか、あるいは達成できそうにない情報のことを言います。技術的な研究プロジェクトの過程で行った実験では失敗を繰り返したものの、最終的な成功に繋がると思われる方向性が明らかになることがあります。望ましい成果を達成できそうにない情報はすべて、会社の営業秘密として蓄積されますが、従業員の中には、その後、ライバル会社に移り、似たような問題について答えを模索している人たちと一緒に仕事をする者も出てきます。そのような場合、会社側は、「ネガティブ・インフォメーションの使用を制限するにはどうすればいいのか」という問題に直面します。Uber社に転職したLevandowskiが、自分がそれまでの数年間Waymo社で取り組んでいた問題にUber社の技術者が取り組んでいることに気付いたとしたら、彼らに対し、「だめだめ、そっちのプロジェクトはあきらめて、こっちのプロジェクトに取り組もうじゃない

か」と言ったかもしれません。そうした重要情報の間接的な使用は、どのように証明すればいいのでしょうか？ 会社の資産としての情報と、従業員の一般的な知識や技術としての情報をどのように区別すればいいのでしょうか？これは簡単なことではありません。

フロア：今、挙げていただいたのは、Levandowski がUber社の従業員で、Uber社は、彼の指示に従って研究の方向性を変更したということです。Uber社の他の関係者には、彼がなぜそのようなことを言うのかがわかりません。この場合、Uber社は、営業秘密を不正利用したというレッテルを貼られるのでしょうか？

Pooley：ええ、責任を負う可能性はあります。ただ、本件においてUber社が採用した方向性が、同社独自の研究に基づくものなのか、それともWaymo社在職時にLevandowskiが得た情報に基づくものなのかはわかりません。わかっているのは、Uber社がWaymo社とは全く異なる技術の採用を決めたということだけです。ですから、Levandowskiがどのような情報を知っていたにせよ、わが社には関係がないと主張できたのです。

フロア：２億4,500万ドルという数字を裁判所はどのようにして導き出したのでしょうか？

Pooley：「裁判所は和解金をどのように算定するのか」ということですね。実は、各企業はリスク分析を行っています。原告と被告の双方が、考えられうる結末を予測し、その結末が現実のものとなる確率を計算しようとするのです。さらに彼らは報告書の専門家の意見を参考にします。リスクを解消することで訴訟を終結させるために、どの程度のリスクなら許容できるのかを明らかにするのです。場合によってはその中間値で折り合いが付くこともあります。裁判がどうなるのかを双方が予想したわけです。

フロア：ということは、裁判を続けるかどうかは、NPV（正味現在価値）、つまり現在の価値といったものに基づくリスク分析で決まるわけですか。

Pooley：ええ、他の交渉と全く同じプロセスです。

Morton：おそらく当事者は、和解に向けての話し合いを行っていたのでしょうね。解決策が見つかるまで、双方がいろいろな提案や要求を行ったのです。

Pooley：興味深い話を聞いたのですが、今回は仲裁役がいなかったそ

うです。双方の企業が直接話し合うなんて、珍しいことですよ。私の経験から言うと、こういう事例では双方が非常に感情的になっているので、和解を実現するためにはプロの仲介者が必要なのですが。

フロア： DTSAは、連邦裁判所で訴えを起こす場合の唯一の根拠なのですか？これまでのことを知らないものですから。州裁判所でも同じようなことはあるのでしょうか？

Pooley： いいえ、州裁判所の場合はかなり違うでしょうね。今回は特許に関する請求があったため、連邦裁判所で裁判が始まりました。結局、特許に関する請求はすべて認められませんでしたが。したがって、かりに営業秘密の窃取に関する補充的請求が、州法のみに基づいて提起されたとしても、裁判官は、その請求を連邦裁判所で審理するという判断を下すことができたでしょう。今回はDTSAに関する請求も併せて行われていたので、この点は問題になりませんでしたが。

Morton： 付け加えたいことがあります。Pooley弁護士は反対かもしれませんが、私には、別の裁判所でも同じ結果が出たのかどうかわかりません。たとえば、今回排除された損害額評価の専門家は、連邦裁判所で審理された他の多くの事件では専門家証人として証言をしています。

Pooley： その通りです。つまり、この損害額評価の専門家は、かわいそうに、裁判官の意見の中で大恥をかかされました。今回の事件でいくつも学ぶことがあったのは、担当の裁判官が、裁判の様子を詳しく話しているからです。おかげでこの事件は、私たちにとってとても興味深いものになりました。他の連邦裁判官は、ほとんどこんなことはしません。ただし、州裁判所が最も違うのは、裁判官が、最初からトライアルに至るまでの過程を、重要な部分を省くことなく行うという点です。被告が、トライアル前に訴え却下のサマリ・ジャッジメントを勝ち取ることは、連邦裁判所よりも州裁判所の方が難しいのです。その結果、州裁判所では、陪審の前でトライアルが開かれる可能性が高くなるわけです。

フロア： 営業秘密の不正利用を根拠に、特許侵害の請求はできるのでしょうか？営業秘密に関する質問というよりも、特許に関する質問になりますが。

Pooley： ええ、この意味ではね。不正利用に関して裁判を起こし、そこで明らかになった事実に基づき、被告の行為が特許侵害にあたることが

証明される場合には、特許侵害の請求を加えることができます。これとは逆のことが起こる場合もあります。たとえば、私の知る限りでは、当初は特許をめぐる訴訟だったにもかかわらず、ディスカバリーで、被告が知るはずのない情報を知っていたことから、その被告が特許侵害のみならず、情報の不正利用に関与していたことが明らかになり、結局、不正利用に関する請求が加えられた事例が数件ありました。

Morton： 他の場合も考えられますよね、特許は公開されますが、公開前は秘密ですから。つまり、その情報が公開される前であれば、それを誰かが不正利用し、使用することも可能なわけです。また、特許になったとしても、1 つの情報について特許と不正利用両方の請求を行うことはできるでしょう。

フロア： 確認ですが、企業が新入社員に対し、前の勤め先が特許侵害をしていたかどうかを聞くのは不適切な行為ですよね。

Pooley： 聞き方によりますよ。前の勤め先が何をしているのかについての情報は、機密情報に該当する場合もあればそうでない場合もあるし、また秘密保持契約（NDA）の適用を受ける場合もあればそうでない場合もあります。したがって、従業員が事実上自由に開示できる情報もあります。状況次第ですので、尋ねる側は周辺の事情を考慮する必要があるでしょうね。

Morton： たしかに、多くの人が雇用契約を結んでおり、通常そうした契約ではその従業員の名前が記載されている先行特許の有無について明らかにするよう求められます。その特許は明らかに公開されていますから。

２．DTSA の成立によって営業秘密の風景は変わるか？

(1) 救済

Morton： では少し議論を進めて、DTSA とそれに伴う救済について話し合っていただきます。差止めや差押えについては皆さん、あまりご存知ないと思いますので、簡単に説明させていただきます。まず、DTSA では 3 種類の暫定的な救済が認められています。それは、山根先生が先ほど少し触れてくださった緊急差止命令（temporary restraining order: TRO）、暫定的差止命令（preliminary injunction）、そして一方的差押え（*ex parte* seizure）

の3つです。

① 緊急差止命令（TRO)

緊急差止命令（一般にTROと略して呼ばれています）は、基本的に短期間の差止めです。この命令の場合、最初に被告側に通知する必要はありません。本来この差止めは、暫定的差止命令に関する審尋が開かれるまで現状を維持する目的で行われます。つまり、連邦裁判所では、裁判所に申立てがなされ、14日間の延長が認められる場合を除いて、この差止めは14日間しか認められません。またよくあることなのですが、被告が、ディスカバリーの時間を増やすために、期間の延長に同意する場合があります。先ほどお話ししたように、原告は、この差止めについて最初に被告に通知しなくてもいいのですが、通知しなかったことについて、説得力ある理由を裁判所に伝える必要があります。こうした準備作業は、書面で行わなければなりません。

② 暫定的差止命令

Morton： 次に、終局判決に先だって発令されるのが、暫定的差止命令です。これも、現状維持のために発令されます。またこの命令は、いわゆる回復不能な損害、つまり金銭的損害賠償では十分に補うことのできない損害の発生を防ぐためのものです。たとえば、あなたが自動運転車にLiDARを搭載する新しい方法を開発したところ、その技術が突然、インターネットで公開されたとしましょう。そうした行為で生じた損害を回復するのは不可能です。一般にこの命令は、他者に対して何らかの行為を禁止するものであって、何らかの行為の遂行を義務付けるものではありません。

暫定的差止命令が認められるためには、原告は、自身が本案で勝訴できることを証明する必要があります。つまり、原告勝訴の確率が5割以上、通常、51%はあるということです。また原告は、回復不能な損害を被る恐れがあることも証明する必要があります。やはり、金銭的損害賠償では不十分でなければなりません。しかも、回復不能な損害は差し迫ったものでなければなりません。つまり、損害が数年後に発生するというのではなく、すぐに発生する恐れがあるということです。この命令が発令される場合としてよく引き合いに出されるのが、情報が公になることで、企業の評判やグッドウィルに傷が付く場合です。裁判では、被告が被る不利益と原告が被る不利益を比較し、原告側の主張がどの程度妥当するのか、どのような

回復不能な損害が発生するのかについて検討が行われます。そして、こうした複雑な比較衡量に基づいて、差止めの発令が妥当かどうか決まるのです。さらに裁判ではしばしば、「差止めは公益に資するか」という点が検討されます。これは難しい問題です。なぜかと言うと、企業同士の裁判では、一般市民が利益を有する可能性がないからです。一般市民が利益を有する典型例としては、ウォーターゲート事件、当時のペンタゴン文書事件があります。あの当時、一般市民にはウォーターゲート事件について知る必要性がありました。ですからあの事件は、一般市民が利益を有する事例になるわけです。

③ 一方的差押え

Morton：　一方的差押えは、DTSAで新たに導入された救済制度です。差止めが、これまで州裁判所において、営業秘密に関する典型的な事例でたびたび発令されてきたことはご存知の通りです。これに対し、一方的差押えは新たな制度であり、DTSAの制定時に大きな話題となりました。ただし、これまでに差押えが認められた例はわずかしかありません。この差押えは特別な状況でのみ認められるので、当然と言えば当然です。これについて考えるのは興味深いことです。と言いますのも、すでに差止めが、ある種の特別な救済として考えられているからです。この差押えの場合も通知は不要です。一般に裁判所は、差止めの場合と同じ基準を採用していますが、両者の違いは、差止めが適切でない場合に限って一方的差押えが認められるという点です。これは、被告が実際に差止命令に従うとは裁判所が考えていないという意味です。原告は、この差押えを申し立てる場合に、被告が不正な手段で営業秘密を取得または使用したことを証明する必要があります。不正な手段の具体例としては、従業員が、競合する会社を立ち上げるために情報を盗む場合や、競合他社が、原告と契約を結んでおきながら、原告との競争に勝つために、その情報を使用する場合が挙げられます。

第1部で山根先生が議論したBlue Star v. Coleman事件[4]は、一方的差押えが認められた数少ないケースです。Blue Star社は石油・天然ガス業界の企

[4] Blue Star Land Servs., LLC v. Coleman, No. 5:17-cv-00931-R, Doc. 10 (W.D. Okla. Aug. 30, 2017).

業で、同社の元従業員数名が、約2万件の文書ファイルをDropboxにダウンロードしました。この行為は、Levandowskiが行ったとされる行為よりも悪質です。山根先生がおっしゃったように、裁判所はDropboxのアカウントのほか、コンピュータ、スマートフォン、タブレットを差し押えて管理下に置きました。また差押時には、差止めの場合と同様、被告に対し、連邦保安官にパスワードを開示し、機器を提出することを義務付けました。

山根： 1つお伺いしてもいいですか。TROや暫定的差止命令でも一方的差押命令と同じこと、つまりDropboxアカウントの差押えはできるのでしょうか。

Morton： ほぼ同じことができると思いますよ。ただし、Dropboxアカウントについては、Dropbox社の協力が必要なのでどうかわかりませんね。通常、差止めの相手方は当事者の一員でなければなりませんが、Dropbox社は当事者の一員ではありませんから。したがって、Dropboxアカウントを差止対象にすることは難しいかもしれません。制度上は可能だとしても、手続上は難しいのではないでしょうか。この辺りは私にはよくわからないので、Pooley弁護士、あなたの考えを聞かせてくれますか?

Pooley： 差押えについてですか?

Morton： ええ、差押えと同じことが、差止めでもできるでしょうか?

Pooley： 差止めで何らかの行為をやめさせるために、連邦裁判所で連邦民事訴訟規則第65条を使うか、州裁判所ならその州の法手続を使うことが可能かと言えば、その答えはイエスです。ただし、差止命令を執行するために、警察に来てもらうことはありません。一方的差押えの利点とは、予告なしに、銃を携帯した保安官を同行させることができるという点にあります。このような抜き打ち行為の現場に居合わせたことがあります。DTSAに基づく差押えではありませんが、それと似たようなケースで、捜索令状のようなものはありました。差押えが行われると知った時の被告の驚きようといったらありませんでした。ただし、ほとんどの場合、通常の連邦民事訴訟規則に基づいて行われる差止めで、同じ救済を執行してもらうことは可能です。なぜかと言えば、差止令状が送達されれば、相手側は、記録を破壊しても、逃げとおせないと気付くからです。結果として、必要なものはすべて手に入るのです。DTSAに基づいて一方的差押えの発令を認めてもらうのはかなり大変です。この2年間でこの命令が発令されたの

はわずか6、7件程度にすぎません。

Morton： それは仕方ないでしょうね。差押えは、稀にしか行われない特別な救済だと考えられていますから。通常の差止めでは、被告がこれに従わない場合には原告側は法廷侮辱罪という救済を受けることができます。実際に私が関わった営業秘密をめぐる事件では、差止命令に従わなかった複数の被告に対して法廷侮辱命令が下されたことがあります。

Pooley： 刑務所に入れられた被告はいたのですか？

Morton： いいえ、暫定的差止命令に従わない場合に認められるのは罰金までででしたから。

④ なぜ一方的差押えの活用率が低いのか？

Morton： ここまでの議論をまとめると、原告に差押命令が認められるのはきわめてまれなケースであるのに対し、営業秘密をめぐる多くの事例では、TROや暫定的差止命令が申し立てられており、しかも認められるケースが多いということですね。では、それはなぜなのでしょうか？

Pooley： 一般に、裁判所が比較的簡単にTROの発令を認めるのには2つの理由があります。まず、一方の当事者から提出された証拠がきわめて説得力のあるものだということです。そこで語られる事実関係は、相手方が非常に悪質な行為を行ったことを示唆するに十分なほど詳細なものです。ですから、裁判官としては、何らかの手を打とうという気になるわけです。もう1つの理由とは、通常、TROが、被告が現在行っている行為を短期間やめさせるためだけのものだからです。私たちは、次の審尋が開催されるまでの間、既存の状況を維持するという意味で、これを「現状」維持のための措置と呼んでいます。ですから裁判官は、自分にはあまり劇的な行為は期待されていないと考えるわけです。こうした理由から、裁判官は、「よし、この申立てには理由がありそうだ。じゃあ署名することにしよう」と決断するのです。

山根： 今の点については私も同意見ですが、一方で、一方的差押えの申立率が伸び悩んでいるのはなぜでしょうか。一方的差押えがDTSA最大の目玉と位置付けられていたことに照らしますと、認容されるかどうかはともかく、もっと多くのケースで申立てがなされることが期待されていたようにも思うのです。しかし実際には申立件数自体が少ない。私の調べた限りでは、DTSA施行後の2年間で一方的差押えの申立てがなされた件数

は21件程度にとどまっています。この数字は、TROの申立件数に比べると格段に少ないわけですが、このように一方的差押えの申立件数が伸び悩んでいるのは要件が厳格だからでしょうか、あるいは一方的差押えに対して裁判所が敵対的な態度を取っているからなのでしょうか。

Morton： その両方だと思います。思うに、裁判所は、一方的差押えに慣れていないのではないでしょうか。州裁判所には、差押令状やそれに似た手続がありますが、ほとんど使われていません。つまり、裁判所にとっては差止めという救済方法の方が使い慣れているので、差押えよりも認めやすいのです。

Pooley： 表現は違いますが、いろいろな裁判官からそれと同じ話を聞きました。たとえば、「一方的な申立て(*ex parte* applications)は嫌いでね。他方の当事者が出席しないのに、申立てを認める気にはなかなかなれないよ。だから、相手方の行為があまりにも悪質なことがきわめて明白な場合にしか一方的な申立てを認めないことにしている」といった具合です。しかも、DTSAで規定されている一方的差押えの要件は非常に厳格です。申立件数が少ないのはそのせいだと思います。ハードルがあまりにも高すぎますよ。それに、先ほどお話ししたように、連邦裁判所で、連邦民事訴訟規則第65条か、あるいは州の差止手続を使えば、合理的な結果を得ることができますからね。

(2) 域外適用

Morton： では、域外適用ないし域外的管轄権(extraterritoriality)の議論に移りたいと思います。Pooley弁護士、このテーマ全般についてお考えをお聞かせいただけますか?

Pooley： わかりました。これはちょっと複雑かもしれませんが、前段階として、少し理解しておかなければならないことがあります。まず、米国の法律によれば、連邦法は国外ではなく国内でのみ適用されることになっています。これが前提、つまり一般的なルールです。ただし、法律案を可決する際に、議会がその法律の域外適用を意図していることが明白な場合、裁判所はその意図を尊重することになります。DTSAを採択した際、議会は域外適用について具体的に述べませんでした。しかし、この法律の2つの規定で、議会は、わが国の営業秘密の不正利用が外国で発生する場

合であっても常に、わが国の経済および雇用の喪失に影響が及ぶことを明確にしています。私たちは、これはとても重大なことだと考えています。そして、外国における不正利用の状況について、定期的に議会に報告がなされることを望んでいます。

第１部でも説明がありましたように、DTSAは連邦経済スパイ法（Economic Espionage Act of 1996: EEA）の一部として制定されました。EEAの第1837条（18 U.S.C. § 1837）は、「本章に定める規定は、次に掲げる場合には、合衆国外において生じた行為に対しても適用される。(1)当該犯罪行為者が合衆国市民もしくは永住許可を受けた外国人、または合衆国または州の法律に基づき、もしくはその監督の下に設立された組織である場合、または(2)当該犯罪を助長する行為が合衆国内でなされた場合」と規定しています。DTSAのもとで域外適用が問題となったある事例で、担当の裁判官は、この第1837条がDTSAに基づく民事訴訟手続にも適用されると考えました。それが正当だと判断したのです。他の裁判官も同じ判断をするかどうかはわかりません。と言いますのも、第1837条は、もともと刑事規定として制定されたものだからです。実際、本条は、犯罪（offense）について、そして犯罪行為者（offender）について述べています。これらは、犯罪行為（criminal behavior）に関する用語です。第1837条が民事訴訟にも適用されるとなると、行為者の一人、つまり被告の一人が米国市民であるか、または被告のいずれかの行為が米国内で行われた不正利用に関連する場合には、日本で行われた不正利用について、米国で訴訟を提起できることになります。

ほかにも２つの可能性が考えられます。１つは、裁判所が、この規定を刑事規定としてのみ捉えて、域外での適用を認めず、その結果、DTSAが米国内においてだけ適用されるというものです。しかし私の考えでは、この規定が域外にも適用されるか否かについて、裁判所は次のように述べる可能性の方が高いように思います。「DTSAを可決した際に、議会は、外国における不正利用が問題だと考えていると述べており、この法律を域外にも適用する意図を明確にしている。したがって、DTSAは、合衆国憲法と矛盾しない形でその管轄権を認めることができる限りは、いかなるケースにも適用されるだろう」と。これはわかりにくい言い方ですが、要は、裁判所は第1837条を民事訴訟にも適用する可能性が高く、私たちは一定の限

度で域外的管轄権を手にすることになるだろうということです。ただし、確実なことはまだわかりません。

フロア： こうした救済が海外で適用された事例をご存知ですか？米国判決が海外でも効力を持つとか、 拘束力を有するとかいった事例を？

Pooley： それは、外国でできるかもしれないことに向けての長い道のりの第一歩のようなものです。もちろん、外国における不正利用を根拠に米国でDTSAに基づく請求を行う人は、米国判決に基づいて何をしようかとじっくり検討するか、あるいは被告の中に米国内に資産を有する者がいるかどうかを確認するでしょう。しかし、いつも懸念されることがありまして、どの国も、国内法の国外適用を主張する時は常に、他国の裁判所の反応を気にせざるを得ないのです。わが国の裁判官が、域外適用を積極的に主張しようとしないのもそのためです。

Pooley： 1つ具体的な事例を挙げるとすれば、2011年に連邦巡回区で判決が下されたTianRui事件[5]が有名でしょう。これは、不正利用がもっぱら中国国内で行われた事件でして、米国企業から営業秘密のライセンスを受けている中国企業の従業員が、その企業を辞めてライバル企業に移る際、当該営業秘密を持ち出したという事件です。転職先の企業が当該営業秘密を用いて製造した製品を米国に輸出しようとしたことから、米国国際貿易委員会（International Trade Commission: ITC）が営業秘密の不正利用事件として取り上げました。本件の不正利用の行為地はもっぱら中国でありましたが、ITCは、当該侵害品を米国国内に輸入する行為に対してこれを差し止める措置を講じました。そこで、このITCによる輸入差止措置の妥当性が連邦巡回区で争われたのです。連邦巡回区はこう述べました。「ITCの判断に問題はありません。私たちは、米国の国内産業に損害を与える恐れがあることを理由に、そのような輸入差止措置ができます」と。しかしそうは言っても、ITCが主張する管轄権は財産に対するものであって、人に対するものではありません。ですから、依然として疑問は残ります。つまり、DTSAに関する判決が出たとして、それに基づいて何ができるのか、ということです。この問題については今なお答えが出ていません。

Morton： 原告が中国で損害賠償を求めようとしたら、かなり違った結

[5] TianRui Group Co. Ltd. v. International Trade Com'n, 661 F.3d 1322 (Fed. Cir. 2011).

果になったでしょうね。

Pooley：　ええ。私は、域外適用の問題を考えている人たちにいつも次のような質問をするのです。TianRui事件と同じような事実関係の事件が起こった場合、それに対して米国の連邦裁判所は管轄権を有するのだろうかと。おそらく答えはイエスでしょうね。ただし、はっきりとはわかりません。わかっているのは、議会もこうしたケースを想定していたということだけです。DTSA法案の審議が行われていた時、私は議員たちにこんな質問をぶつけました。「この法律は域外にも適用できることを意図しているとなぜ言わないのですか？」と。すると、彼らはこう答えました。「この議会では無理だ」と。その理由は、そうすることで連邦政府が権限を濫用しているような印象を与え、きわめて多くの人がそれを好ましくないと考える恐れがあったからでした。ですから私たちは、それを間接的に行うことになったのです。

Morton：この規定が頻繁に適用される可能性があることから考えると、日本企業が巻き込まれるリスクがあるのではないですか？

山根：　私はあると思います。とりわけ第1837条（18 U.S.C. § 1837）をDTSAに基づく民事訴訟にも適用したT&S Brass & Bronze Works, Inc.事件判決[6]は、日本企業にとって大きなインパクトがあるように思います。たとえば、日本企業Ａがシリコンバレーのテック系ベンチャー企業Ｂを買収し、その技術情報を日本で使用したとしましょう。もしＢ社の保有する技術情報が、Levandowskiのケースのように、米国企業Ｃから不正取得した営業秘密であったとしますと、Ｃ社はＡ社に対し、営業秘密侵害を理由に米国で訴訟を提起する可能性があります。すなわち、Ａ社はＢ社買収時に当該不正取得の事実を知っていたか知りえたはずであるにもかかわらず、当該技術情報を日本で使用する行為はＣ社の営業秘密の不正利用に該当するというわけです。

特に先の判決によれば、第1837条の第２項もDTSA訴訟に適用され、米国外の不正利用を助長する行為が米国内でなされていれば、当該米国外の

[6] T&S Brass & Bronze Works, Inc. v. Slanina, 2017 U.S. Dist. LEXIS 68155 (D.S.C. May 4, 2017). 同判決の基礎になっているT&S Brass & Bronze Works, Inc. v. Slanina, 2016 U.S. Dist. LEXIS 186427 (D.S.C. Dec. 20, 2016)［治安判事の勧告意見］も参照。

不正利用に対する域外的管轄権が米国の連邦裁判所に認められることになります。そのため、上記の例のように、A社が日本で使用する技術情報が米国で不正取得されたものであったような場合には、A社に対するDTSA訴訟の管轄が米国の連邦裁判所に認められる、ということになりそうです。

このように、買収した米国企業の技術情報に不正取得された他社の営業秘密が含まれるような場合には、当該情報を日本で使用する場合であっても、第1837条第2項を根拠に、米国で提起される営業秘密訴訟に日本企業が巻き込まれる可能性が高いように思われます。このことは、侵害の成否にかかわらず(つまりA社がB社買収時に当該不正取得の事実を知っていたかどうかにかかわらず)、日本企業が米国の連邦裁判所に出廷し、ディスカバリー等にも応じなければならないことを意味します。こうした応訴の負担は、日本企業にとって大きなリスクと言えます。

Pooley： 全く同感ですね。まさしくそういうことが起こると思われます。しかも、ディスカバリーに応じなければならないというリスクのみならず、米国で莫大な額の損害賠償判決が下されるかもしれないというリスクもあるのです。ちょうど1ヵ月前に、テキサス州の郡裁判所で行われた営業秘密事件の陪審裁判で、7億600万ドルの損害賠償を命じる評決が出ました[7]。州裁判所でのちょっとした訴訟でもこの額です。

3．オープンイノベーションと営業秘密

Morton： では次に、オープンイノベーションのテーマに移りたいと思います。ここからは、ある企業が別の企業と提携する際のリスクと、それについてどのようなプランを立てればいいのかについて考えます。この場合によく行われるのは、秘密保持契約と雇用契約の締結です。企業側が検討すべき具体的な問題はいくつかありますが、Pooley弁護士、この点についてご意見を聞かせていただけますか？

Pooley： 一般論として、外国の提携先やサプライチェーンを構成する

[7] Title Source Inc. v. HouseCanary Inc., f/k/a Canary Analytics, Inc., No. 2016-CI-06300 (73rd Dist. Ct., Bexar County, Tex. Mar. 14, 2018).

業者と取引を行う企業が、自社の営業秘密情報のリスク管理で行うべきことは、彼らが最悪の行動に出ると想定してプランを立てることです。たとえば、サプライチェーンを構成するメンバー全員が自社の機密情報の取扱いに慎重でないと想定して、サプライチェーン全体のセキュリティを向上させる措置を考える必要があります。さらに、自社の情報を守るために、提携先に義務付けるべきことを、できるだけ契約に盛り込むようにしなければなりません。具体的には、提携先の企業に対し、各従業員との間で秘密保持契約を結ばせ、その中で、保護すべき当事者として、顧客の名前を明記するよう義務付けることです。なぜなら、多くの国では、営業秘密を盗んだとされる人物と直接契約を結んでいなければ、どの企業も救済を受けることができなくなるからです。さらに、提携先に対しては、従業員の誰かが辞める際には知らせるように義務付けておく必要があります。そうすることで、その人物が、退職後どこに勤めるかがわかるからです。これらはいずれも、管理上の負担に照らして情報の秘密性がどれほど高いのかによって左右されます。しかし、情報の重要度が高くなればなるほど、それを保有する企業としては、提携先がその情報をどのように扱っているのかを常に把握しておきたいと思うものです。

また、情報を保有する企業には、提携先にどのような手続を課す場合であれ、その監査（audit）を提携先で行う権利があります。そして、実際に監査権を行使するのです。私の知る限りでは、特に中国で多くの企業が利用しているのが、違約金に関する規定です。差止めという救済手段が認められにくかったり、事実審で差止めがなかなか認められなかったりする中国ですが、違約金を科す命令に関しては裁判所が非常に積極的に認めてくれる場合がよくあります。そこで、何か問題が生じた時には、相手方企業が自社に5,000米ドルを支払うことを契約に規定するのです。このことは、地元のアクターに対し、相手方企業に開示した自社の営業秘密が不正利用されないように監視する義務を課すうえで重要なインセンティブとして機能します。こうした規定を契約に盛り込み、地元で優秀なマネジャーと弁護士を見付け、地元当局の実情を把握し、問題が発生した時の対応策を準備しておくのです。地元警察の最高責任者を知っておくのも得策です。さらに、保有する情報が失われるというリスクだけでも軽減するために、情報を保有する企業は、自らが必要と考えるほかのあらゆる実践的対策を

講じるべきです。

Morton： 私のクライアントの多くは、そうした契約を厳格に管理しています。これらの企業は、営業や技術を担当する部署に対しこうした契約の締結を認めていましたが、弁護士は、かなり後になるまでそのことを知りませんでした。ただし現在では、会社側が、秘密保持契約を結ぶ前に弁護士に相談し、法律上の承認を得ておくよう営業担当部署に義務付けています。これは大切なことです。なぜかと言えば、秘密保持契約には、自社にとって不利な条項が盛り込まれている可能性があるからです。その１つが、秘密保持契約に明記される期限です。18ヵ月後には公表されるであろう相手方企業の情報の開示を契約でいつまでも禁じられるという状況に陥りたくはないでしょう。つまり、秘密保持契約を締結する際に、法律上の適切な助言を仰ぐことが重要なのです。

Pooley： まさにMorton弁護士のおっしゃる通りです。よく聞かれるのは、「営業秘密をめぐる企業間の紛争で最も多い原因は何か」という質問です。それは、間違いなく、秘密保持契約を適切に管理できなかったことです。ですから、多くの人たちは、それらが事実上契約である場合には、それらを１つのフォームとして理解します。そしてMorton弁護士が指摘した通り、ある企業が保有する情報が18ヵ月後には公表されることが見込まれる状況で秘密保持契約を締結する場合、大きな問題になるのが期限です。その時点では、契約に基づいて情報の開示を受けることは効果的でした。ただし、負担が増える場合もあります。つまり、情報の取扱いにきわめて厳しい制限が課せられる場合、情報を受け取る側は、管理上きわめて大きな負担を負うことになるからです。Morton弁護士の指摘はとても重要です。急に契約を結ばなくても済むように、これについては一括して管理する必要があります。

フロア： 先ほどお話のあった営業秘密の監査についてですが、それはどういうもので、どのように行われるのですか？

Pooley： 私が言った監査とは、いずれかの企業が保有する秘密情報を受け取る側、すなわち情報を保有する企業の提携相手であり、他国に所在し、その情報を開示されたサプライチェーンの重要な構成員か、またはイノベーションのパートナーのいずれかに対するパフォーマンス監査です。情報を保有する企業は、情報の受け取り手と契約を結び、それに基づいて

彼らには特定の行為、たとえば開示された情報を特定の場所に保管し、その情報にアクセスできる人物を制限するよう義務付けます。情報を保有する企業としては、自身の情報がどのように扱われるのかについて、相手方に出向き、監査を行う権利を持ちたいと常に考えています。そしてその権利を行使したいとも考えています。もちろん、その権利をどのように行使するのかについては、契約の条件や両者の関係によって異なります。たとえば、予告なしにそうした権利が行使できる場合もあれば、それが認められない場合もあります。たとえばAppleは、新製品のデザインを秘密にしておくために、サプライチェーンが採用しているシステムについて、きわめて厳しい監査プログラムを策定しています。そして今や、誰もがそれに慣れています。つまり、私がお話ししたのは、いわゆる一般的な監査ではありません。時々、この言葉を使いたくないと誰もが思います。ちなみに私は、企業が自ら保有する情報を保護するために合理的措置を講じているかどうかを調べるうえでどのような点に注意すべきかを説明する際には、「ギャップ分析（gap analysis）」という表現を使います。

Morton：　おそらくPooley弁護士も賛成してくれると思いますが、企業は、自分たちの社内プラクティスについて調べる場合と同じ注意を払うべきですよね。特許とか特許出願とか、特許出願までの経過をたどるということになると、発明者のノートに対して細心の注意が払われます。しかし、自分たちの営業秘密がどのようなものなのかを知ろうとする際には、必ずしも同じような注意が払われているわけではありません。彼らは、営業秘密の一覧表を作成したり、監査を行ったりするべきでしょうか？

Pooley：　ええ、一般論としてはね。資産としてのそうしたデータの慎重な管理は、きわめて重要になっていますから、この一般的な問題については、Morton弁護士と同意見です。ただし、私としては、「監査（audit）」とか「一覧表（inventory）」といった言葉は使いたくないです。なぜかと言うと、自己の資産としての情報について把握するために、かつて金物屋が店内にあるボルトやねじの数を調べる際に店を閉めていたように、企業も業務を停止しなければならないかのような印象を与えますから。顧客と取引を行う際に、秘密情報の管理にどれくらい費用をかけてもらえるのかについて、現実的に評価しておく必要があります。ただし、そうは言っても、そのためには、取引先がどのような管理をしているのかということや、そ

うしたプロセスがいかに重要なものであるのかということを把握しているマネジャーが必要になります。合理的措置とは何かという一般的なテーマについて議論しようと思うと、そのためだけにセミナーが1つ開けますよ。

4．秘密保持のための合理的措置に関する日米比較

Morton： ご指摘ありがとうございます。さて、最後のテーマは、日本と米国の比較分析です。秘密保持のための合理的措置に関して、両国に違いはあるのでしょうか?

山根：日本の秘密管理性要件とDTSAの秘密保持のための合理的措置要件とは、要件としては似ています。しかし、その裁判所における運用実態を比較してみますと、両国の間には大きな差異があるように思われます。

第1部の報告で述べましたように、日本の営業秘密訴訟では、2006年から2015年の10年間で見ますと、秘密管理性要件に基づく原告の請求棄却率が51%にのぼります。つまり全訴訟のうちの実に半分のケースにおいて、秘密管理性を欠くことを理由に原告の請求が棄却されています。棄却事例に占める割合で見ましても、秘密管理性の欠如は棄却事例の58%を占めており、突出した棄却理由をなしています。

一方、DTSA訴訟では、施行後の1年間で見ますと、秘密保持のための合理的措置要件に基づく原告の請求棄却率は5%にとどまります。棄却事例に占める割合で見ましても、合理的措置の欠如は棄却事例の11%を占めるにとどまります。

このように、日本の秘密管理性要件とDTSAの秘密保持のための合理的措置要件の運用実態を比較してみますと、本要件に基づく原告の請求棄却率に関しては10倍の差が、棄却事例において両要件が占める割合に関しては5倍の差があることがわかります。

Pooley： その数字は衝撃的ですね。米国と日本にそれほどの差があるなんて思いもよりませんでした。実は、わが国で合理的措置がとられなかったことを根拠に原告の請求が棄却される事例は、30〜40年前、つまり私がこの仕事を始めた1970年代の方がはるかに少なかったのです。当時、裁判官はこう言ったものです。「ええ、たしかにそれは要件だが、最低限の

要件だ」と。なぜでしょうか？裁判官は、こうした事例では、ある人物が情報を不正に取得したとして訴えられ、その確たる証拠があることを常に知っているのです。そしてその同じ人物あるいは同じ会社が、原告（被害者）はあまりにも多くの情報を保護せずに放置していたと主張するということも。裁判官にしてみれば、それはまるで、自動車泥棒が、盗んだ自動車の持ち主は鍵を差したままだったと言っているようなものです。したがって当時は、合理的措置が講じられたかどうかという争点に、裁判官が時間をかけるのはきわめてまれなことだったのです。

現在では、特に連邦裁判所の裁判官は、この争点についてかつての裁判官よりも時間をかけて精査しています。そして今の方が、以前よりも裁判官は少し懐疑的になっています。しかしそれでも、この点について被告に有利な終局判決が出た事例として私が知っているのは、たぶん10〜12件ぐらいか、それよりも少し多いぐらいでしょう。私が自著で引用したいくつかの事例について考えてみても、米国は日本と同じレベルではありません。山根先生のおっしゃる通りだと思います。もしわが国の訴訟において半数の企業しか営業秘密を管理できていないと言われれば、米国企業は司法制度に不満を持つのではないでしょうか。

Morton：　そもそも車に鍵を差し込んだままその場を離れた企業だけに問題があるというわけではありません。社内のありとあらゆるものに――ペンや紙にも――鍵をかけるべきだという極論になりますから。社内のすべての文書に秘密という表示を付けたからといって、合理的措置を講じたことにはならないでしょう。裁判所はそれに対して懐疑的になるでしょう。

Pooley：　まさしく、そうなるだけの理由があります。裁判官が適切に調べれば、彼らは、データセキュリティの管理システムが、事実上、従業員を管理の対象にしていることに気付くでしょう。従業員が取り扱っているデータがどのような性質のものか、それにはどのような制限が課されているのかに関する厳しい研修や、なぜそのデータにアクセスしたのかに関する厳格な理由開示手続など、従業員とのコミュニケーションのすべてが、損害の主たる発生原因である従業員に対応するためのものです。ですから、あらゆる文書に㊙の印を付ける以外に何もしない、あるいは従業員にすべてが秘密だと言う以外何もしないというのであれば、その企業は、重要なものとそうでないものを区別する手段を従業員に提供していないことに

なります。その場合、従業員はきわめてずさんで不注意になる傾向があります。過剰な表示が大問題になりかねない理由はそこにあるのです。

Morton： つまり、今回の議論で覚えておくべき点は、従業員教育を徹底し、営業秘密と営業秘密方針を維持すべきだということですね。

フロア： 先ほどスライドにあった東京地裁の事例[8]についてお聞きしたいことがあります。質問は2つあるのですが、まず、これはB to Bの事例ですか、それともB to Cの事例ですか？

山根： B to Cの事例です。

フロア： なるほど、よくわかりました。このような質問をしたのは、複数の企業が顧客リストの一部をネットで公開しているからです。もし先の事例がB to Bの事例であれば、従業員が秘密保持義務を負っていたとしても、リストに秘密であることを示す表示がなかったのですから、秘密管理性を否定した日本の裁判所の判断は合理的であるように思えました。最初はそう感じたのですが、先生のお答えでB to Cの事例だということでしたので、その部分についてはよくわかりました。ですから、質問はこの1問だけで終わらせていただきます。

フロア： Pooley弁護士のお話は過剰な表示についてでしたが、従業員が退職する際に交わす契約についてお聞きしたいと思います。彼らが署名する契約には、「会社在職中に得たいかなる秘密情報についても、転職先で使用しません」という旨の記載があります。営業秘密として保護されないような情報を、こうした契約によって手厚く保護することはできるのでしょうか？

Pooley： 一般論として、特に私が実務家として携わっているカリフォルニア州法の場合、営業秘密に該当しない情報を契約で保護することはできません。ただし、これはそれほど重大なことではありません。と言うのも、営業秘密として認められるためのハードルが非常に低いからです。営業秘密の要件を見た限りでは、営業秘密として保護されるものは、第一次不法行為法リステートメントが作成された1939年当時と同じではありません。今ではより広範なものが保護されます。さらに現在の法律によれば、何らかの価値を有する情報は、それがインターネットで検索できるもので

[8] 東京地判平成18・7・25平成16(ワ)25672「訪問看護名簿」。

ない限り、事実上すべて保護の対象になるのです。つまり、ハードルが非常に低くなっているわけです。

５．最後にひと言

Morton：最後に、今日お越しの皆さんにぜひ覚えて帰ってもらいたいことがあれば、教えてください。

Pooley：そうですね、私が強調したいのは、営業秘密の管理に関する点です。これには、私が弁護士になりたての頃の考えが関係していましてね。実は、1978年にある事件を担当した時に、私はこんなふうに思い至ったのです。「これまで営業秘密をめぐる事件をいくつも担当してきたが、そうした事例には１つの共通点がある。誰かが馬鹿げたことをやらかすんだ」と。どの事例も必ずそうです。たとえばLevandowskiは、ばれるはずはないと思って、機密ファイルをすべてダウンロードしました。高度な営業秘密管理が正しく行われた場合、それは古典的な意味でのリスク管理プログラムにほかなりません。とりわけ、こうしたプログラムと一緒にしっかりとした従業員研修プログラムを実践すれば、情報の喪失、破壊、混入（コンタミネーション）をどんな方法よりも確実に防ぐことができるでしょう。実は、私が危惧しているのは、ほとんどの企業が、十分な注意を怠ったがために、そうしたチャンスを逃しているということです。企業には、コンプライアンスに関してほかにもやるべきことがたくさんあります。しかし、今や自分たちにとって最も重要な資産になったデータの管理に、企業は依然として十分な注意を払っていないのが現状です。

Morton：おっしゃる通りです。営業秘密はひとたび流出してしまえば、もう何の価値もありませんから。訴訟を起こして、その回復を図ろうとすることはできても、損害賠償はなかなか認められません。私が言いたいのは、企業は入社初日から従業員の研修を続けるべきだということです。そして、退職時のプログラムを用意しておくことを忘れてはなりません。退職時のプログラムの一環として、きわめて重要な技術情報を知っている従業員が退職する前に、彼らのコンピュータのデータのコピーを取っておくといいでしょう。営業秘密の存在を忘れてはいけません。秘密情報が適切に扱われるように、職場では従業員を単独で作業させないようにしましょ

う。自社の営業秘密についてしっかりと管理する必要があるのです。

山根： 先ほども述べましたが、日本における最大の課題は、秘密管理性要件の運用のあり方だと思います。この要件の文言自体は日本と米国とでそれほど変わりませんが、その運用の実態に関しては、両国の間で大きな差異があります。しかし、少なくともこの10年ほどは、日米両国の法運用の実態を比較する研究はほとんどなされてきませんでした。そのため、多くの人にとって、米国から見た日本の法運用の特徴を認識することが難しかったように思います。

その意味でも、まず重要なことは、2006年から2015年までの10年間、日本では全訴訟の半分のケースにおいて秘密管理性の欠如を理由に原告の請求が棄却されていること、棄却事例に占める割合で見ても秘密管理性の欠如は棄却事例の58%を占めており、突出した棄却理由をなしていること、この割合はDTSA訴訟の5倍にのぼり、日本の営業秘密訴訟の大きな特徴をなしていることを認識することだと思います。そのうえで、こうした法運用を今後も維持することが営業秘密をめぐるわが国の法政策として望ましいのかどうかを考える必要があるように思います。今回の第1部報告および第2部パネルディスカッションの議論が、こうした目的にとって少しでも参考になるところがあれば幸いに思います。

Morton： ほかに何かご質問は？

フロア： とても細かい話になるかと思いますが、特許化のプロセス、つまり先ほどお話のあった、特許が公開される前の非公開の期間についてお聞きします。クライアントがこのまま特許を取得して技術を公開します、あるいは出願を取り下げて技術を非公開にします、と言ってきた時、当該技術の社内での取扱いについて、どのようなことをアドバイスすべきでしょうか？

Pooley： まず、公開日の数週間前の時点で、このまま特許を取得するのか、それとも出願を取り下げるのか、つまり技術を公開するのかどうかをもう一度よく考える必要があります。公開することにした場合、資産であるデータの全体的な管理を行っている状況であれば、当然、あなたは、「よし、いよいよ公開だ。これから私たちは、これを商品化し、実際に売り出し、もしも自分たちで使うつもりがない場合には他者にライセンスを与えるために何をすればいいのだろう？」などと考えるでしょう。それ以

外にもあなたは、この特許に必要であり、特許に関連している営業秘密として現在保有している付帯情報は何かとか、この発明を確実に実現するために必要なノウハウとは何かについて調べるでしょう。このようにして、多くの情報を一括管理するのです。企業法務に携わる知り合いの多くから聞いたところによれば、かつて社内の特許委員会で行われていた特許化のプロセスでは、委員たちが、「じゃあ、これについて特許を取得しよう、あれについて特許を取得しよう」というふうに決めていたそうです。そしてそれ以外のものについては、それ以降、見向きもしませんでした。もっとも、今はそのようなことは決してありません。たとえ特許が取得できそうになくても、このプロセスで検討対象になったものについては、必ず次のような質問に答えを出さなければならないのです。それは、「なぜ特許が取得できないのか？もしこれで特許を取得しないのなら、ほかにどのような形で使えるのか？どういうふうに保護すればいいのか？そして担当者は誰にすべきか？」こうした点について議論が行われるわけでして、公開に関しても、こうした議論が行われるべきです。

Morton： ありがとうございました。以上で本日のパネルディスカッションは終わりにしたいと思います。ディスカッションにご参加くださった皆さまが有意義な時間をお過ごしいただけたとすれば幸いです。（拍手）

［付記］
本研究はJSPS科研費JP18H05216、JP17K13664、JP15H01928の助成を受けたものです。