技術情報が漏洩したら

～第３回技術情報防衛シンポジウムパネルで お伝えしきれなかった内容も含め～

モデレーター	久留晴夫（キヤノン株式会社）
パネリスト	小栗宏之（警察庁）
	林いづみ（桜坂法律事務所）
	鈴木嘉浩（株式会社デンソー）
	加藤達夫（凸版印刷株式）

議題

1．「営業秘密をめぐる実務」　（桜坂法律事務所　林　いづみ弁護士）

2．刑事手続きと民事手続き

3．「株式会社デンソー様のご経験、そこから学んだこと」
（株式会社デンソー　知的財産部　部長　鈴木　嘉浩様）

4．平成27年　不正競争防止法改正について

5．いわれのない訴訟に備えて

の付いているページは、前回のパネルではお伝えしきれなかった内容になります。

刑事、民事についての日本の現状について

林先生

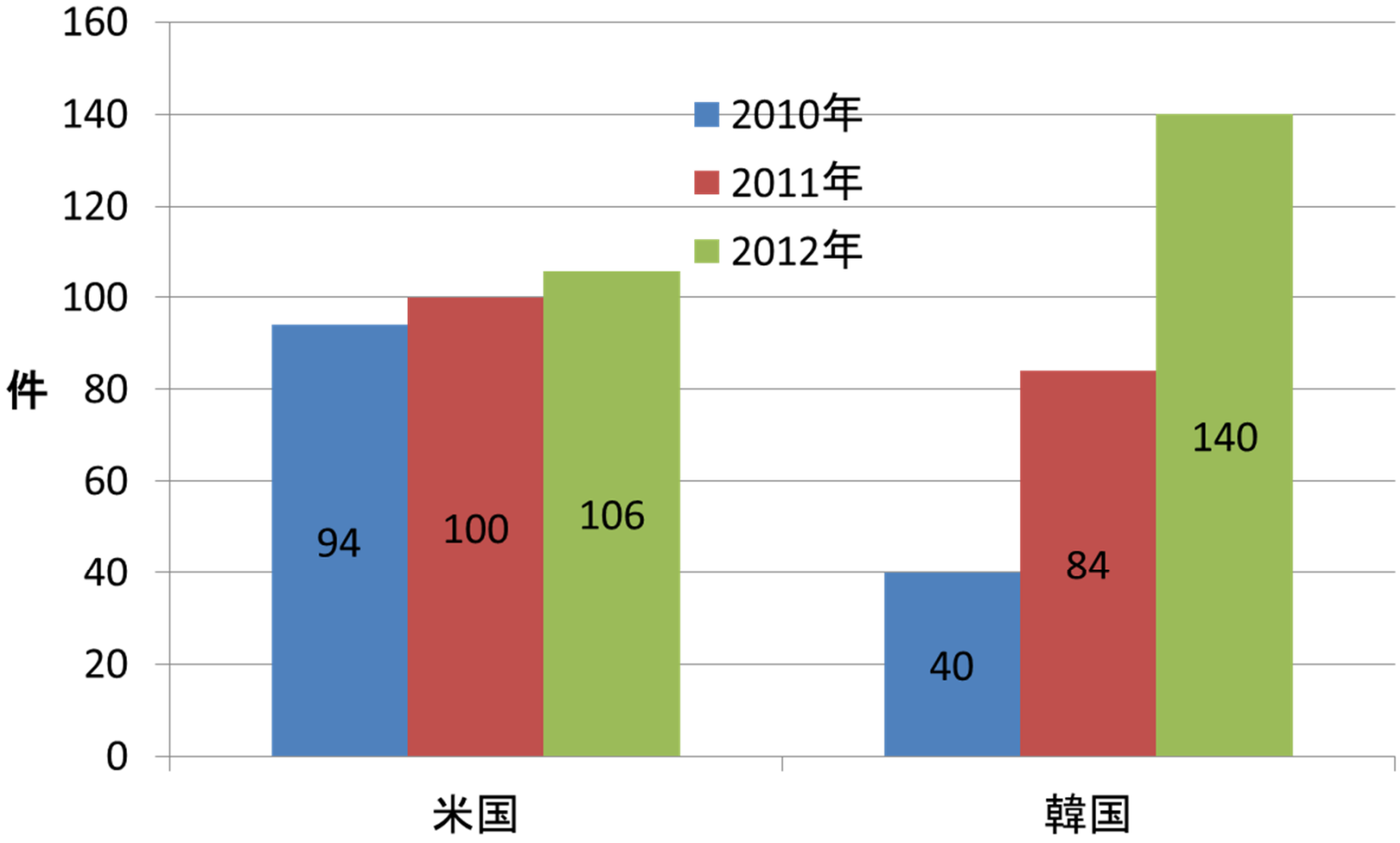
最高裁判所の判決データベースで「営業秘密」で検索すると240件ヒット。
営業秘密に関する事案があって、弁護士まで相談が来て、さらに、訴訟を提訴し、
裁判上の和解も取り下げもなく、最終的に判決に至るのは氷山の一角。
最近のサイバーアタックとは別に、昔ながらの事案、つまり、会社の待遇に不満を持つ
定年間際の社員が会社を辞めて起業したり競合会社に再就職するというレベルの
相談は全国的に非常に増えているという実感。

小栗さん

警察庁に報告のあった件数では、平成25年は相談が13件で、検挙は5事件。
平成26年は相談が29件で検挙は11事件。
　なお、この検挙は、逮捕したものと書類送検したものの合計件数。
（書類送検には、事件として厳しいと判断したものも含まれている。）

久留からアメリカ、韓国のデータの紹介

（参考）米国・韓国の捜査件数



営業秘密関連事案の捜査件数

韓国警察庁の営業秘密関連事案の摘発件数

おとり捜査について

小栗さん

おとり捜査とは、警察官がその意図を秘して第三者に犯罪を行わせるような
働きかけをして、犯行に及んだところを検挙する捜査方法。

日本国内では、薬物事犯や拳銃事犯などで、嫌疑はあってもその他の手法では犯人を
特定できない場合などに行われる場合がある。

ただし、この場合であっても、全くその気のない人間に働きかけて、
犯行を決意させる犯意誘発型捜査は認められておらず、
薬物を売りたいと相手方を探しているような人間に、買い取るからと働きかけて
表に出てきたところを逮捕する機会提供型に限って認められる。

いずれにせよ、必要性がどこまであるかによるのが、営業秘密侵害事犯でも、
売り込みを図っている相手に、身分を隠して買い取るよ、
と持ちかけることはありうるのかな、と。

実際に営業秘密の漏えい問題について

- **警察への相談は、どういう段階でどこにしたらよいか？**
- **その際、警察として取り上げるか否かの判断にどのような要素が考慮されるか？**
- **被害額は考慮されるのか？**

タイミング的には、「盗まれた。」ということがある程度推定できた段階で速やかにお願いしたい。

その前に、民事でいくか、刑事でいくかの会社として判断されると思うが、
時間が経てば経つほど証拠というものは散逸していくので、緊急事態ということで
迅速に意思決定をしていただきたい。

相談先としては、都道府県によって生活経済課であるとか、生活環境課であるとか
名称が違うが、警察本部の不正競争防止法違反事件の担当課にお願いしたい。

警察が取り上げるかどうかは、被害額がどうかというより、本当に事件なのか、
言い換えると、現時点で証拠はどれくらいあって、
これからどれくらい集まりそうかが重要。

- **営業秘密侵害事件においても、犯人を特定できなくてもご相談してかまわないか？**
- **相手の会社が国内会社の場合と海外会社の場合で状況は変わってくるか？**

犯人が誰かがわかればそれに越したことはないが、必ずしも必要ではない。

ただ、泥棒の場合、部屋が荒らされているなど、物が盗られた＝犯罪があったことは明白で、
届けがあればすぐに被害届を受理するが、営業秘密事案の場合、これはどうなっていますか、
こんな証拠はありますかというようなやり取り（告訴相談という。）をしてから、告訴の正式受理となる。

このやり取り（相談）に要する期間が長くなるか、短くなるか、最終的に受理できるか、受理できないかは、ケースバイケースだが、最初の警察への届出段階で、事実関係がすべてわかっていなければならないということではない。警察としては、最初からすいませんと謝る相手はいないという前提で、では、それをどうやって覆していくかという見方をする。会社として訴えようという結論を出したということは、「独自開発」と言い張られても、そんなことはあり得ない、と判断したということであろうから、まずは、そういった所を詳しく聞かていただことになる。

その上で、例えば、ログが全くないので立証ができないということがわかれば、その理由をお話しして、告訴を受理しても処罰は難しいことを、と説明をさせていただくことになる。

なお、外国会社が最終的に使用したとしても、その前段の領得が国内で行われた場合などは、国内で収集できる証拠で領得部分の犯罪の立証はできるはずなので、海外会社が絡んだことが、
イコール刑事告訴は無理とはならないと考える。

➢ 知財における知財高裁のように、営業秘密侵害事犯は一律どこか一か所でということはないという理解でいいか？

警察は都道府県警察が活動単位の基本で、管轄権がある。
したがって、本社がある場所である、実際に持出が行われた場所である、
犯人がいる場所であるといった、関連がない都道府県は捜査をすることは
できないことになっている。

こうしたことから、INPITの営業秘密110番から転送された事件相談は、
警察庁で管轄権を考えて、対応する都道府県を指定するとの枠組みとしたところ。

実際に捜査をすることを考えれば、証拠が多い場所を管轄するところが
一番適当なわけで、必要に応じて関係場所を管轄する複数県で
共同・合同捜査を行うことになる。

- **刑事として成立するかどうかは、「最低このくらいやっておかないと、そもそも機密管理性の観点で難しい例」として、ログの例がでていたが、そのあたりもう少し詳しく。**

小栗さん

管理性のポイントは、持ち出した側が、秘密の情報なのか、それ以外の情報なのかを後づけではなく、持ち出した時点で理解し得たかどうかになると思われる。

例えば、ログを取っていることを知っていた場合と知らなかった場合を比べてみると、トレーサビリティーについてはどちらも変わりはないが、それが秘密と理解し得たかという点では差がある。

秘密だからログを取ってますよ、ということをしっかり伝えた、相手もそういう話を聞いていたということを立証すれば、秘密管理性を認定してもらう上で有効。

ただ、秘密管理性は、総合判断、実態判断ですので、秘密表示をする、分別管理をする、持出管理をする、そして、こうしたことをそれぞれの現場でしっかり守ってもらうということが大切。

➢ 現実問題として膨大なログの保管にはコスト面で負担になる。どのくらいの期間保管しておけばよいか？

警察としては、やはり時効の7年間は保管してもらいたいと考える。

ただ、なぜログをとるのか、それは、流出してもすぐにばれるよと言うメッセージによる
抑止効果と、いざ流出した際の犯人特定のためということを考えると、
陳腐化した情報を持ち出されても、訴えようということにはならないと思うので、
そういったサイクルを考えて、ログを廃棄することもあり得るのかな、と考える。

- **非親告罪化により、今後刑事手続きに進む事案が増えると思うが、技術情報漏洩捜査で、警察に提出した情報は、裁判等で公開される恐れはないか？**
- **ポイントは最初から弁護士と一緒にすすめるということになると思うが、その際に気をつけることは？**

林先生

刑事訴訟手続きの特例として秘匿決定のしくみがあるが、その対応のためにも
事件が発覚した最初から弁護士と一緒に準備して、捜査機関への相談に臨むべき。

なお、NBL（1049・5月１日）に秘匿決定の実務について詳細に触れられていることを紹介

加藤Q：
企業として今後刑事と民事を具体的にどのように使い分けるべきかという点が気になる。
たとえば、情報を不正取得したと思われる個人を刑事告訴し、その状況を見ながら転職先の企業に対して民事訴訟を提起するといったことが考えられる。
民事・刑事をどのように使い分けることが望ましいのかをもう少し具体的に教えてほしい。

林先生

刑事手続きを利用するメリットの一つとして捜査機関による証拠収集を期待できるという点がある。

加藤さんのご質問にあるような、まず、情報を不正取得した者を刑事告訴する場合、
図利加害立証のためには、競合会社へのデータ売却するなどの証拠が必要だが、
こうした、競合会社へのデータ売却目的や売却事実の証拠収集は私企業には困難だが、
捜査機関には可能。

刑事事件の進捗状況に応じてということになるが、刑事事件の証拠を、競合会社に対する民事訴訟において当該営業秘密の「不正使用」事実の立証に使うメリットはあると思う。

小栗さん

理論的には、刑事責任と民事責任は別物だが、警察の立場からすると、例えば、民事が先行していると、呼び出して取り調べしようとすると、民事の一方に肩を入れているなどとすぐに抗議されて呼び出しに応じないなど、正直、やりにくい。また、民事で判決が出るまで闘った人間は、逃走や罪証隠滅のおそれが疎明できないので、逮捕という選択肢もなくなることになる。

これは検察庁の話になるが、民事で負けた、相応の支払いをしたということが、起訴判断に影響しているのではと感じたケースもある。

できれば、刑事でいくと決めたなら、その結末を待ってから民事に移ってもらいたいと思うが、絶対にダメとまではいえない。

なお、刑事事件の方が証拠の吟味が厳しいので、刑事を念頭に揃えた証拠は民事でも有効に使えると思う。

最終的に刑事はあきらめて民事一本でいくということになっても、それまでは、刑事でいくことも念頭に、入手経路や改ざん等がないことを明らかにするように準備を進められたら良いのではないか。

➢ 証拠の話が出ましたが、「刑事における証拠」について

小栗さん

刑事の場合、立証責任は検察側ひいては警察にあり、どんなことを言われても
揺るぎない程度の証明をしなければならない。

例えば、無理矢理に供述させられた、改ざんされたと被告が主張すれば、
それを完全に打ち消さなければならない。

民事の場合、相手方が欠席した場合が典型だが、どんな主張であっても、
相手が反論しなければそのことは認めたことになり、認めた以上は
証拠はそれほどいらない、という世界なので、やはりハードルの高さは相当違うと思う。

デンソーの事案

1．2007年。
機密の図面が漏洩した事案。アクセス権を持つ中途採用者が
自分のパソコンにダウンロードして持ち出し

2．従来紙ベースの管理が利便性のため、人的チェックの機会が欠落して
行ったことが原因

機密管理の基本概念を性善説から「Trust but verify」に変更

①各個人の権限を必要最小限に制限し、利用実績を監視
②入手したデータのメール送信／記憶媒体書き出しを制限
③データの社外への持ち出しルールを厳格化
④やむをえず持ち出す情報は暗号化し万一の流出を防止

※以降、不正流出が疑われる事案は発生していない。

➢ **この事案は刑事的には21条1項3とか4とかに該当すると思うが、当時の「不正競合目的で」という条件では字義どおりに取ると該当するかどうか厳しい感じがするが、現在の「図利加害目的で」においてはどうか？**

小栗さん

質問は、平成21年改正で、「不正の競争の目的」が現行の「図利加害目的」になって、競合他社が関与しない単純な加害目的での行為や、そもそも競争関係が考えられない外国政府のためにした行為も処罰対象となった、処罰範囲が拡大した、といわれている部分のことと思います。

拡大したと言われても、警察的には、この「目的」という部分は、単に持ち出しただけでは犯罪ではありませんよ、正当な理由がなくて持ち出しても犯罪とは言い切れませんよ、目的があって持ち出して初めて犯罪ですよ、という捉え方をしています。

先ほど、この図利加害目的での抗弁も多いとお話ししましたが、競合会社に渡した、までは不要ですが、どこかに売り込みを図ったであるとか、インターネットで晒そうとして準備していた、というところまでは立証が必要となるので、図利加害目的になって極端に立証が楽になったとは考えていません。

「図利加害」に該当するかどうか、というところもそれほど簡単な判断ではないことと理解した。

- **凸版ではどのような対応をしているか？社内の認識は？**
- **業務の中で「顧客の情報」を扱うということで、自社情報との比較で特段の配慮をしてるか？**

加藤さん

当社ではダイレクトメールの発送や各種カードの作成などの業務を行っており、個人情報を含めお客様からお預かりする情報がたくさんある。そのため情報の管理が非常に重要。
お客様の情報については、営業秘密としてだけでなく、個人情報保護の観点からも情報の受取から社内での保管、返却までのルールが明確に定められ、書類やデータを安全性の高い専用エリアに保管することで漏洩を防ぐ仕組みをつくっている。

また、電子部品の回路等の設計図面データのような機密性の高いデータに関しては、専用の保管場所を定め、アクセス権を持った人以外はデータに触れないような管理をしている。

こういった管理を全ての情報で行うことは難しいので、特別な扱いが必要なデータ以外は、各部署で機密性を有する情報を抽出し情報管理表にて管理。管理表には情報の種類、重要度、秘密管理区分、管理場所、利用可能者、管理責任者等を記載してあり、社員はこの管理表に基づき情報を扱い、定期監査で管理レベルが適切か、取り決めが守られているかなどをチェック。

一方、自社の技術情報に関しては保護すべき情報の特定が難しいうえ、複数の社内関係者が共有したり、共同開発先や得意先への開示も必要になることから画一的な管理は難しい。

社内の認識については、このような情報管理に加えて具体的事故事例の紹介を含めた教育を定期的に行っており、認識は低くはないと思っている。ただ、こと情報管理に関しては性善説に立ってはいけないと感じているので、サーバーのアクセス制限やログの管理も行っている。

➢ **デンソーの機密管理の海外のグループ会社などを含めた、グローバルなガバナンス体制は？**

鈴木さん

最も重要と考えている図面管理については、日本と同様のシステム（考え）で対応。
大事なことは、会社毎（生産会社が多いので、その必要な製品図面等について）に、
情報制限を行うこと。

必要と考えていることは、定期的な監査。
上記システムがしっかりと機能しているのかどうか？
従業員自身の機密意識が高く維持されているのか？
現地現物でチェックすること。

法改正について

不正競争防止法　これまでの改正経緯

平成2年改正	・営業秘密保護導入
平成15年改正	・営業秘密不正取得等に対する刑事罰を規定
平成17年改正	・一定条件の退職者・法人に対する刑事罰導入 ・国外犯規定導入
平成18年改正	・罰則規定の法定刑引上げ
平成21年改正	・目的要件変更（不正の競争目的⇒図利加害目的） ・領得行為を刑事罰の対象に
平成23年改正	・営業秘密の内容を保護するための刑事訴訟手続の整備（秘匿決定等）

法改正について

今回の改正は、企業の声がだいぶ反映されたものと思うが、
- **法改正までの流れも含め今回の改正について全体的にどう評価されるか？**
- **課題、懸念点などは？**

林先生

私も審議会委員の一人だったが、刑事手続については審議会の告書提出後に決まったもの。率直に言って、他の知財法にもない没収規定がはいり、不正競争防止法に章が3つも増えたことには驚いた。

発展途上国と違って、日本の警察・検察は中立性については懸念する点はないが、営業秘密といっても、色々なタイプがあり、高度な技術的に関する営業秘密について、企業側のみならず、相談を受ける県警本部にも周知が課題。

民事関係では5条の2の推定規定の導入がポイント。
被告側としては防御のために、コンタミリスク対策が重要になる。
改正法では、適用対象が限定されているが、原告側による違法取得の事実の立証の程度、被告側の反証の程度は、裁判所の運用次第なので、今後の事案の蓄積を注目したい。

法改正について　～未遂罪～

未遂罪は「犯罪の実行の着手」がありその結果うまくいかなかったということが前提になるとのことだが、

- **「情報をダウンロードすべくウイルスを仕掛ける」というような例は「実行の着手」に当たる、つまり未遂として罪に問えると考えていいか？**
- **それとも、「ダウンロードが実行されたがそれがうまくいかなかった」というところまで必要なのか？**

林先生

これからの実例を見る必要があるが、対象となるのではないか。
また、不正アクセスの証拠はあるが、アクセス先に営業秘密は存在しておらず
ダウンロードされていないという場合なども対象になると思う。

法改正について　～非親告罪化～

- **一部には、被害企業の意思とは別に事件がすすんでしまうのでは？という懸念がある。**

小栗さん

理論的には、親告罪は公訴提起の条件であって、捜査開始の条件ではないので親告罪であろうがなかろうが、告訴があろうがなかろうが、警察は捜査はできる。

しかし、捜査の実務を考えると、例えば、ある企業の情報を外国企業が狙っているらしいという話があったとしても、本当に情報が盗まれたのかは、その企業に聞かなければわからない。

また、別の事件でどこかの企業から情報を持ち出したということがわかったとしても、秘密管理性については実態判断なので、その情報が現場でどのように扱われていたのかは企業側の協力がないと立証はできない。つまり、警察が勝手にことを進めることは現実的にできない。

ただ、暴力団が絡んだ事件などで行われているのだが、当初は届けないという意思表示がなされたとしても、警察が被害者を説得して届出をしていただくということもあるので、こうしたお願いをさせていただくことはあり得ると思う。

法改正について　～推定規定～

そもそも推定規程が適用されるためのハードルも高いわけだ、企業の心配としては「営業秘密をはきださせることを目的に」提訴され、被告になるケース。
要するに、被告として反証する際、自社の営業秘密が原告にしられてしまう危惧がある。

- **これに関連して、民事手続きにおける特則として不正競争防止法10条から12条に秘密保持命令の規定というのがあるが、そもそもこの命令はどういうもので、実際に活用されているのか？　実際に命令が出された事例は？**

林先生

実際は、秘密保持命令を求め、その対象となる人物の特定において下手に関連分野の技術者などを指名すると、コンタミネーションを排除できず、
場合によっては業務から外さざるを得ない
などということもあり、正直活用しやすい制度とはいえない。

法改正について　～犯罪収益の没収～

林先生

改正法の19条の2では、没収に関する手続は、この法律で定めるものの他、政令や最高裁判所規則で定めることとされている。

また、改正法の21条12項では、没収できないときや、当該財産の性質や、使用の状況、当該財産に関する犯人以外の者の権利の有無その他の事情から、これを没収することが相当でないと認められるときは、その価額を犯人から追徴することができると定められている。

また、没収に関する手続等の特例として、改正不正競争防止法に第7章、8章、9章が新設された。第三者の財産の没収の場合は、その第三者は被告事件の手続への参加が許されること、裁判所は、没収保全命令や追徴保全命令をして、財産の処分を禁止できること、日本で没収対象になる行為が外国で行われた場合の外国の刑事事件についえ外国粗没収若しくは追徴の確定裁判の執行などの共助の要請があった時は原則としてそれに応じることなどが定められている。

いずれにせよ、実行に際してはいろいろはハードルがあると思われるので実例を待ちたい。

参考

損害賠償について、関連する話として4月に出たアメリカのデュポンーコーロン事件の刑事裁判で、興味深い部分がありましたので紹介。

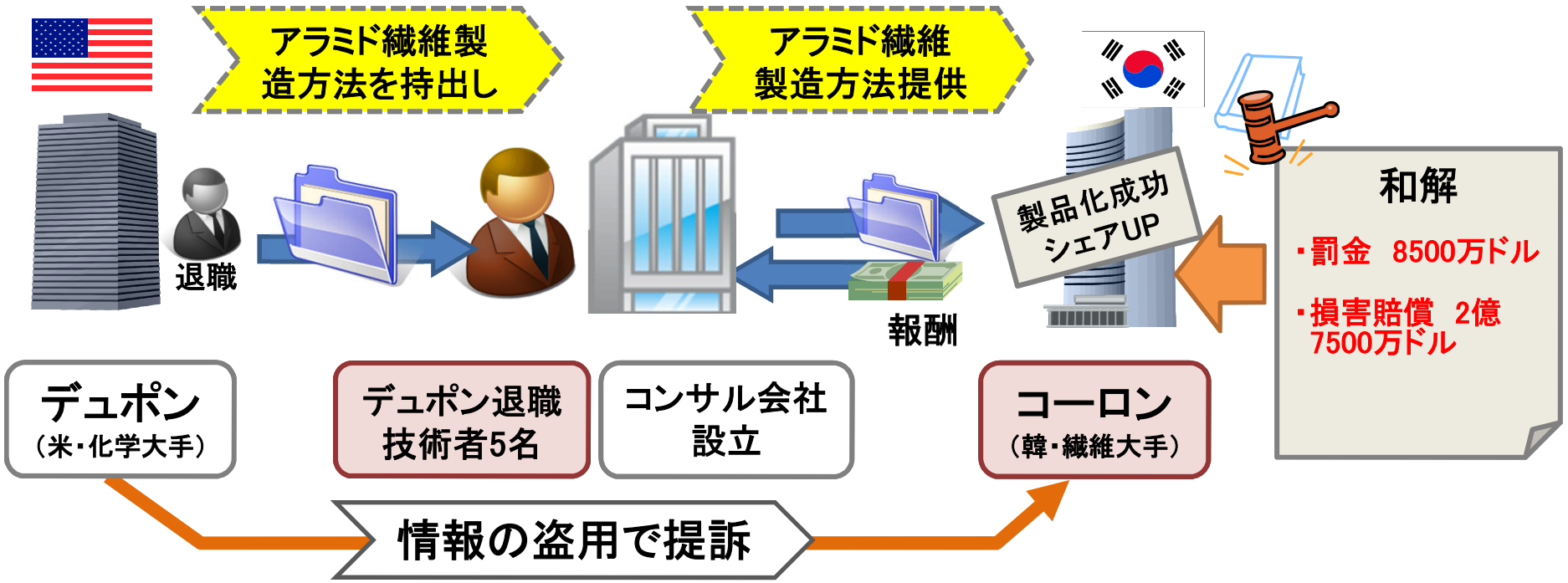
この判決において、罰金とは別に275ミリオンドルの「損害賠償」の支払いが命じられているが、特筆すべきは、これが刑事裁判の中での被害者に対する損害賠償であるという点。

restitutionという被害者に対する刑事上の損害補償の制度で、民事における損害賠償額の算定において、同じ内容の損害については、restituionの分が勘案されて相殺に対象になる(こともある)とのこと。

被害者の立場からすればわざわざ別途民事で戦わなくても「損害賠償」を得られるのはありがたいと思う。

米国 営業秘密侵害事例

経済スパイ法適用 【デュポンvsコーロン事件】



刑事訴訟	・2010年10月、コーロン社及び同社役員5名が起訴される （※米国経済スパイ法に依る） ・2015年4月コーロン社は共謀してデュポンの営業秘密を盗んだことを認める（和解）
民事訴訟	・2011年9月、バージニア州の連邦地方裁判所で判決（上記） ・コーロンが連邦控訴裁判所へ控訴 連邦地裁判決を破棄、差戻しの判決（2014年4月） ⇒係争中

➢ 今回の改正で心配な点は？

加藤さん

被告になるリスクがどの程度増えるのかといった点。

自社の情報漏洩の心配もさることながら、昨今のように人の流動化が進むと、途採用した人材から意図せず他社の情報が自社に入り込む恐れがある。また、共同開発や業務提携なども増えており、このような場合にも他社の情報が混入する恐れがある。

今後は他社から受領した情報の管理が重要になると感じている。
当社においても、複数のお客様とのお付き合いがあるため、同業種のお客様に対しては営業部門が重複しないような体制をとっている。
一方、技術情報に関しては、現実的にはお客様ごとの技術開発部門を用意するわけには行かないので、日ごろから情報管理には気を使っている。
共同開発先や業務提携先などから入手する情報に関して、これまで以上に注意を払う必要があると思う。

ただし、情報の管理をあまり厳格にしてしまうと事業活動に影響が出るので、そのあたりのバランスが難しいところ。

- **転職の自由との関係もあると思うが、今後は、転職者の受け入れにあたり、前職で知り得た情報の不開示についての誓約書取得に加えて、詳細なジョブインタビューや面談といった追加の実務対応が必要になってくると思う、その他注意すべき点は？**

林先生

前職での営業秘密を聞き出すようなインタビューは当然まずい。
日本企業の定年退職者に対してアジアの企業からそういう内容のアンケートのようなものが送られてくることがあるとのこと。

それが営業秘密侵害になるということを従業員に啓蒙するとともに、
同じ轍を踏んではいけないと思う。

たとえばあるノウハウがたとえば「口伝」で継承され、有体的には固定されていいないものの、そのノウハウが当該社製品の値のかなめであり、完全に記憶だけでそのノウハウを持っている人が退職し、転職先でそのノウハウを「使用」したような場合、刑事罰、民事訴訟の対象にはなるのでしょうか？という質問があった。

- **まず、無形の情報が「営業秘密」として認められる条件はどういうものか？**
- **刑事の場合は、21条1項6号に該当する場合、つまり在職中に他者にオファーするなどした場合のみ該当しうる、ということと理解しているが、民事は？**

林先生

まず、口伝であろうと、秘密として特定されていれば営業秘密には該当する。

民事では、不正競争防止法2条1項7号により、従業員が正当に取得した営業秘密を、不正の利益を得る目的またはその保有者に損害を与える目的（図利加害目的）で、使用又は開示する行為は、営業秘密侵害にあたる。ここでは、刑事の場合の21条1項3号のような横領・複製・破棄仮装という行為の限定はないし、使用又は開示行為が退職前か後かの区別もない。

もちろん、実務的には立証などの目的においても
何らかの形で管理できる形にしておくに越したことはない。

あらためて、いざという時に備えてという点でアドバイスを

小栗さん

相談を見ていると、ログを取っている企業さんでも、退職申出があって調べて初めてわかった、というようなケースが多く、普段ではなかなか気付いていられない企業もあるなと感じている。私事だが山形県警にいたときは情報管理も仕事だったのだが、一定の閾値を超えた回数の機微情報へのアクセスをした者について、その上司から、どんな仕事をさせていたのか、その仕事に照らしてアクセス件数はおかしくないのか、という報告を求めていた。既に実施されている企業さんもあるとは思うが、アクセス回数が一定の閾値を超えたであるとか、休日にアクセスがあったとか、あれっと思ったときには確認をしてもらうようなことをお願いしたいと思う。

また、繰り返しになるが、捜査は警察だけできるものではなく、被害者の協力が不可欠であるということ。自転車窃盗みたいに単純な事件なら、警察に届け出れば、あとは全部やってくれる、ということになるが、営業秘密侵害事犯の場合は、届出すればそれで終わり、とはならないということ。

私も業務上横領などの告訴相談を何件も受けてきたが、その都度、「人一人を訴えて、刑務所に入れようという意思表示ですから、相応の責任をありますよ。」とお話しして協力をお願いしてきた。

これは、逆に言えば、繰り返しになるが非親告罪になっても、警察が勝手に捜査を進められないと言うことでもある。

あらためて、いざという時に備えてという点でアドバイスを

林先生

最低限のポイントとしては、企業として、オープン・クローズ戦略において秘匿化を
選択する以上は、トップダウンで組織として適切に取り組むことだと思う。

実際に取り組むと情報の仕分け段階から現場からは面倒がられるので、
防犯と同じで被害にあうまでは先送りしがち。

社内に営業秘密管理のタスクフォースを作り、地道に取り組むこと。
企業のトップが率先して、その取り組みをサポートすることが必要ではないかと思う。

結び

いざという時にどういうことをしたらいいか、できるか、ということについていろいろお話をうかがってきたが、普段の備えとしては、やはり営業秘密として保護すべきものを重点的に区別し、システム的にログを取るだけではなく、ログを活用するところまで仕組みとして構築したい。

ただ、メリハリが必要。「指針」にも触れられていると思うが、機密が漏えいしないための規定、仕組みと、営業秘密としての保護を受けるための規程、仕組みは若干視点が異なるので、意識して両方の視点をもったマトリックスの体制が大事。

前者を完ぺきにした結果業務に支障が出た。いざという時いまいち役に立たなかった。ということのないようにしたい。2月の「産構審の小委員会による中間とりまとめ」のなかでも、「情報は基本的に使うことが前提であって、盗まれることを避けるために管理しなければならないとしても、あまりに厳格な管理をすると業務効率が落ちるので過度に厳格な管理をもとめるべきではない。」という指摘もある。

いずれにせよ従業員の認識・教育が大前提で、定期的な啓蒙の機会は不可欠。

また、コンタミネーションを防ぐための採用時の注意が、より一層重要になってきたことをいっそう意識しなければならない。

なお、小栗さんのお話にも出てきたように、この2月には、工業所有権情報・研修館（INPIT）に「営業秘密110番」（正式には営業秘密・知財戦略相談窓口）というのができて、営業秘密に関連する相談もすでに50件ほど受けているとのこと。まだ今日現在実例はないようだが、相談事案によっては警察庁につなげる、という機能も想定されているので、そちらもぜひご活用されたい。