

2015年1月15日

明治大学知的財産法政策研究所(IPLPI)シンポジウム

営業秘密保護のこれまでとこれから

文部科学省私立大学戦略的研究基盤形成支援事業（平成23~27年度）

情報財の多元的価値と、創作・利用主体の役割を考慮した知的財産法体系の再構築

「営業秘密保護強化に関する最近の政策展開について」

木尾修文（経済産業省経済産業政策局知的財産政策室室長）

経済産業省経済産業政策局知的財産政策室長の木尾でございます。本日は、どうぞよろしく申し上げます。今日まさに中間取りまとめをしたところですが、産業構造審議会の方で営業秘密の保護強化について、9月から4回議論をやってまいりました。私からは、そこでの議論の中身、あるいは今日、とりあえず中間取りまとめをやらせていただきました、その結果についてご紹介をさせていただきたいと思っております。

早速でございますが、まず情報の流出の現状ということで、私どもの問題意識についてでございます。4つほど事例を書かせていただいております。先ほど棚橋会長からもご紹介がございましたけれども、新日鉄住金の話、あるいは東芝の話、あと下側に、やや毛色の違う話でございますけれども、ベネッセの話、JP モルガンの話を書かせていただいております。

何が言いたいかと申し上げますと、上2つ、新日鉄住金の話あるいは東芝の話というのは、わが国の国富の源泉になるような、そういう重要な技術が外国企業に盗まれましたという事例でございます。下2つについては、サイバー攻撃的な手段であったり、あるいは伝統的な、内部者の犯行によるものであったりして、個人情報が出てしまったと。特にベネッセの話で言うと、報道でご存じの方も多いかと思いますけれども、6次取得者まで、ITで環境の変化もあると思っておりますけれども、情報が転々流通したと。3,000万人分ぐらいの個人情報が漏れたという状況になってございます。

私どもの問題意識としては、もちろん個人情報の部分についても手当てをしていかなければいけないわけでございますけれども、より喫緊の課題として、より重要だと思っておりますのは、上2つに代表されるような技術情報が不正に取得されるということについて、どうやって抑止力を高めていくのかということに最大の問題意識を持ってございます。

その上で、この4事例以外に、わが国において、日本企業でどの程度、こういう情報の流出、営業秘密の流出というのが起こっているのかということでございますけれども、それについて簡単にご紹介させていただきます。

左側の円グラフからまずはご紹介させていただきます。この結果は、若干古いのですが、私どもが2年前にアンケート調査をやらせていただいた結果でございます。回答は約3,000

社からいただいているものでございますけれども、何が申し上げたいかという、今まで、過失も含んでいますけれども、故意、過失で営業秘密、情報が漏れたことがありますかと。そういう質問をさせていただきましたけれども、それに対して、明らかに漏えい事例がありましたという企業が7%弱ぐらいです。おそらく情報流出があったという人も7%弱と。合計で13%ちょっとぐらいの人が、情報漏えいを、おそらくという方も含めて、経験をされていると。これは括弧内の数字に特にご注目いただければと思いますけれども、これを従業員が3,000人超の企業に限定して数字を集計すると、合計で言うと、だいたい約40%の企業が、漏えい事例があった、あるいはおそらくあったというようなご回答をいただいているという状況になってございます。

下側に注3で書かせていただいておりますのは、こちらの方が調査としては新しいわけでございますけれども、昨年9月に帝国データバンクが発表されている調査でございます。これはベネッセの事件の後の話ですが、営業秘密に関する企業の実態調査ということで、回答者数は私どもの調査よりも多くて1万1,000社ということになってますけれども、そちらについても、営業秘密の漏えいの疑いがあるというようなご回答をされた方は10%弱ということなので、若干数字が違うにせよ、いずれにせよ、わが国において、そういう営業秘密の漏えいというものが相当な規模で、大規模で起こっているという状況というふうに思っております。

右側で説明させていただきますけれども、どういう具体的な態様で情報漏えいが起こっているのかということになるわけでございますが、こちらについては、最近、それこそサイバー攻撃的な事案も、特にアメリカなんかで非常に多く報道でも見かけているところでございますけれども、この瞬間、伝統的な形態としては、やはり社員を経由するもの、内部者の犯行によるものが支配的な割合を占めているということでございます。その中でも、中途退職者、中には元々の企業に対する処遇面での不満等々を抱えていらっしゃる方ももしかしたらいるのかもしれませんが、中途退職者による情報漏えいというのがやはり目立つなど。半分ぐらいを占めているなどということになってございます。

右下でございます。営業秘密情報の区分状況でございますけれども、これについて申し上げたいことは、情報漏えいがかかなり大規模に日本で起こっているということに対応して、日本企業、わが国の企業はどの程度の情報管理、営業秘密の管理というのをやっているんだろうかという問題意識でお伺いしたものでございます。結論として申し上げますと、相当濃淡があるなど。色を付けたところで書いてございますけれども、営業秘密を管理する、情報を保護するということになると、まず第1段階として申し上げますと、何が営業秘密なのか、何が営業秘密じゃないのかということとを区分することからスタートするわけですが、そもそもその区分をやっていないとご回答いただいている方が4割弱ぐらいなので、役所も大したことを言える立場でもないわけでございますけれども、なかなか日本企業の中でも濃淡があると。相当ちゃんとやっているところ、ちゃんとやっていないところというのがあるなどという印象を持っております。

その上で、先ほどの棚橋会長からもご紹介があった話の、やや繰り返しになるわけですが、アメリカとか韓国とか、外国の同様の営業秘密の情報についてご紹介させていただければと思います。

左側の上に、アメリカの警察機関だと思えますけれども、FBI が捜査をしている件数を書かせていただいております。下側に、捜査に基づいてということだと思えますが、経済スパイ法に基づいて実際に起訴をしましたという件数を書かせていただいております。お分かりのとおり、特に左上の捜査の件数でございますけれども、年々増えて、直近でデータが取れる 2012 年で言うと、100 件超ぐらいの件数があるということになってございます。ちなみに、ご案内のとおりでございますけれども、日本ではだいたい年間、せいぜい 1 件、2 件、3 件という程度のものなので、そういう意味で言うと、多ければいいというものでは決してございませんけれども、アメリカとの相当な差があると思っております。

右側に、具体的にどういう事例があるのかということをご紹介させていただいております。これは、一定の基準に基づいて客観的にソートして掲載したものではありません。目立つものを載せているということでございますけれども、分かることは、まず漏えい企業、あるいは漏えいした情報の中身として、いわゆる軍事技術とか安全保障関係の技術に全然限定されることなく、民生技術についても国の力の源泉になるような部分が多いかと思えますけれども、そういうものも広く対象になっているということでもあります。タイヤの関係の技術であったり、有機肥料の関係の話であったり、あるいは化学物質の関係の技術であったり、極めて広範な分野の技術がターゲットになっているということでございます。

一番右側の欄に、刑事罰についても書かせていただいておりますけれども、日本と比べた場合に、相対的には違うということですが、アメリカの方はかなり重罰が科されているということでもあります。それこそ一番下のデュポンのケースなんかで言うと、15 年の懲役が科されたりとか、日本では、後ほど申し上げることになるんですけども、営業秘密の関係の実刑判決というものは一件もないという状況でございますけれども、それに比べると、アメリカの方が相対的には重いという状況なのかなと思っております。

ちなみに、この紙には書いてございませんけれども、アメリカの元連邦検事が分析しているレポートによれば、この捜査の件数、100 件ぐらいあるということですが、その半分以上は中国絡みのものであるという報道がございます。

次に、お隣の韓国もこういう分野についてはかなり積極的な取り組みをされているわけですが、そちらについてもご紹介させていただきます。

基本的には、アメリカと傾向としてはかなり似ておりますが、こちらについても、左側に、韓国の警察庁が発表されている摘発件数を紹介させていただいておりますけれども、傾向として読み取れることは、年々増加傾向にあると。直近で、2012 年で言うと 140 件と、アメリカ以上の件数になっているということかなと思っております。

左下に、技術流出の分野を書かせていただいておりますが、お互いがまさに競争力ある分

野とも重なるかと思えますけれども、電気・電子であったり、機械の分野があったり、右側の円グラフでございますけれども、内容で言うと、具体的にはどういう形態の営業秘密が盗られましたかということになると、設計図面が半分ぐらいを占めているという状況にあるということです。

右側に、アメリカの場合と同様に、具体的なケースを書かせていただいております。こちらについても、流出先としては、中国企業とか、あるいは台湾企業とか、外国企業が相当数あるということと、漏えい情報としては、こちらについても同様に、お菓子の製造方法なんかから始まって、かなり広い分野の民生技術がターゲットになっていると。そういうことかなと思ってございます。

その上で、秘密としている情報について、それが漏れてしまうんだったら、初めから漏れることを前提にして、特許にする、権利化するという議論も世の中にはあるわけですが、こちらについては、結論として申し上げますと、まさによく昨今、議論になりますけれども、オープン・クローズ戦略というんでしょうか。技術について、何を特許にするのか、何を特許にしないで隠していくのかということについて、戦略的に取り組んでいきたいと思いますということだと思えますけれども、日本企業における基本的な傾向としては、技術が秘匿化される傾向にあるということかなと思ってます。

昨年後半に私どもが行ったアンケート調査、先ほど申し上げた 3,000 社に対するアンケート調査とは別の調査でございますけれども、このアンケート調査の結果を紹介させていただきます。こちらは、5 年前との比較において、特許要件を満たすであろうと。そう思われる発明について、御社の中であえて特許にする、出願するという選択肢を選ばないで、営業秘密として秘匿化するというものの割合が増えていますか、減っていますかということをお聞きしたものでございますが、そちらについては、増えていると回答いただいた方がだいたい 3 割ぐらいということになってございます。

さらに、右下に、最重要の営業秘密、秘匿技術が仮に漏えいしてしまいましたという場合にはどういう影響がありますかということをお聞きしたデータでございますけれども、約半分ぐらいの回答者数、企業から、経営に致命的なレベルの損害を受けるというご回答をいただいているということでございます。

左側に、ここにいらっしゃる方はご存じの方も多いかと思いますが、特許にするのか、営業秘密にするのか。別にオープン＝特許というわけではなくて、あるいはクローズ＝営業秘密というわけでもないんですけれども、あえて単純化して、オープンの戦略として特許を選んだ場合、クローズの戦略として営業秘密を選んだ場合として、単純化して記載させていただきますけれども、特許については、権利としてはすごく強力ですと。一方で、営業秘密については、いったん漏えいすれば、特にインターネット上に拡散すれば、秘密としては全く無価値になってしまう。それこそ数百億円、数千億円かけて開発した技術の成果であったとしても価値がなくなってしまうということが、特許のメリットであり、営業秘密のデメリットであるということだと思っています。

逆に、特許について、デメリットも当然あるわけで、よく言われる話で言うと、世界中に公開されてしまうと。特に、機械翻訳の精度の向上、機械翻訳については著しく精度が向上しているというふうに聞いてございますけれども、精度の向上もあって、出願公開から、それこそ1週間、2週間たつと、世界中の企業がまねをすることができる、あるいはその企業のその製品の改良のヒントを与えてしまうというようなことがデメリットとしてはあるんだろうなと思ってございます。あるいは、特許の行政手続きというんでしょうか。審査のための費用とか、あるいは登録料とかいう費用は、当然のことながら、かかってくると。それこそ日米欧で特許を取っていけば、1件でたぶん1,000万円単位のお金がかかってくるんでしょうということだと思っています。あと、権利期間終了後、特許の場合は原則20年ですけれども、20年、権利期間を経過したとしたら誰でも使用可能になってしまいますねということだと思っています。

そういう意味で、特許についても、営業秘密についても、メリット、デメリットがすごくあって、技術の性格によって、あるいは事業戦略によって、オープンにするのか、クローズにするのかということをも日本企業は選択をしつつある、戦略的に考えつつあるということだと思っておりますけれども、その結果として、秘匿化をする、営業秘密にするというような割合がどちらかといえば増えている傾向にあると。一方で、それがターゲットになって漏れていく傾向でもあるので、そのバランス対策を考えていく必要があるということだと思っています。

その上で、ややおさらいになってしまいますけれども、営業秘密の保護について、現行の制度はどうなっているんですかということについて、ご存じない方もいらっしゃるかと思いますので、ごく簡単にご紹介させていただきます。

改めてでございますけれども、不正競争防止法で営業秘密の定義をしているわけでございますけれども、私どもの知的財産政策室の方で、所管としては不正競争防止法を担当しているということになってございます。その上で、不正競争防止法上の営業秘密に仮に該当するような情報であれば、民事・刑事両面で法的に保護されるということになっております。

具体的に申し上げますと、典型的なものとして、営業秘密に該当することが多いものを例としてご紹介させていただきますと、設計図などは典型的です。あるいは、製造原価であるとか、実験データであるとか、原料、特に化学関係の塗料とかの原料ですけれども、その配合比率とか、あるいは、われわれの世界では文系の営業秘密とか言ったりするんですけども、顧客の情報や販売マニュアル、あるいは財務データ、仕入先リスト、この辺りについては、必ずしも自社のデータではなくて、取引先であるとか下請先のデータなんかも最近はかなり多いようでございますけれども、そういう多種多様な営業秘密がございます。

その形態も、もちろん情報ということですけども、その情報が具体的に取っている形態も、紙の場合もあれば、金型みたいな、営業秘密が化体したものみたいな場合もあれば、

あるいは機械そのものに化体しているという場合もありますし、あるいは特に最近、増えてきているのが、電子データとして営業秘密が保管され、管理されるというケースが圧倒的なものとして増えつつあるということだと思っています。

その上で、営業秘密の定義でございますけれども、よく言われる 3 要件がございまして、有用性、非公知性、秘密管理性という要件がございます。この中で一番問題になるのは秘密管理性なわけでございますけれども、有用性については、有用な営業上の情報であることということで、何が言いたいかと申し上げますと、保護の対象として、例えば有害物質の垂れ流しの情報であるとか、あるいは脱税の情報であるとか、そういうものは法的な保護には値しないということでございます。

2 目、非公知性の要件ですけれども、これは保有者の管理下以外では一般には入手できないと。これについてもいろいろ解釈はありますけれども、典型的に該当しないものとして申し上げますと、例えば刊行物、雑誌に載っている情報、本に載っている情報みたいなものについては、非公知性は満たさないと。誰でも知っているようなもの、誰でも知り得るものについては、法的な保護には値しませんということでございます。

最後、秘密管理性ですけれども、秘密として管理されていることという単純な表現を書かせていただいておりますが、法文上、不正競争防止法の条文としてはこういう条文になってございますけれども、これについては、後ほどご説明させていただきますけれども、なかなか議論が尽きないところがあって、何をすれば秘密管理として認められるんですかと。書類であれば、マル秘のスタンプを押せばいいのか、その紙を金庫の中に入れてもいいのか、金庫に鍵も閉めなければいけないのか、金庫を開けられる人が何人ぐらいいるのか、何をどこまでやればいいのかということについて、実務をされているような企業からは、いろいろな悩みの声が寄せられているという状況でございます。

営業秘密の定義、有用性、非公知性、秘密管理性ということをご紹介させていただきましたが、その 3 要件を満たす場合については、不正競争防止法上の措置ということで、冒頭、中山先生からご紹介がございましたが、あくまで不法行為法の特則、民事法上は基本的には損害賠償しかできないということが原則になるわけですが、不正競争防止法の場合には、民事規定として、侵害の差止、予防の他にももちろん賠償もできます。あるいは、その賠償についても、損害額の推定規定があったり、あるいは民事訴訟の手続きの中において、秘密保持命令の形で、公開の法廷で漏れないようにするというようなこともあり得ることになってございます。あるいは、刑事の措置としては、先ほどの説明とも若干重なりますけれども、凶利加害目的という限定がある下で、不正な取得・使用あるいは開示といった行為について処罰しますと。

ちなみに、現行の法定刑として申し上げますと、今、法定刑についても、産業構造審議会では議論をさせていただいたところがございますけれども、現行が、懲役が 10 年以下、罰金が 1,000 万円以下、法人が 3 億円という形になってございます。こちらについては、先ほどご紹介したような新日鉄住金のケースで言うと、当事者の主張によればということです

けれども、情報を漏らした元社員の方は数億円の金銭をもらっており、利益とは概念として若干違いますけれども、その損害賠償の請求としては 1,000 億円を請求していると。先般、報道もされていましたが、東芝のケースで言うと、和解金として 300 億円超の和解がされた。そういう状況の中で、産業界の方々からは、懲役 10 年、あるいは特に罰金でございませうけれども、1,000 万とか、法人重課の 3 億円というところについて、抑止力として十分だと思いますかというところについては、いろいろな議論があるということでございます。

あと、念のためでございますけれども、この図利加害目的、私は今年の 7 月からこの仕事をさせていただいているんですけども、そもそも読み方が分からなくて、ズリって読むのかと思ったんですけども、正確にはトリと読むらしいです。この図利加害目的、要は自己または第三者の利益を図るとというのが図利です。加害というのが、分かりやすい言葉で言えば、リベンジみたいなことをイメージしていただいたらいいんだと思いますけれども、もともといた企業に対して、一種の不満を持って報復をする、復讐をする、リベンジをするという、そういう目的の下での行為を処罰すると。逆に、公益通報であるとか、「残業のために情報を持ち帰りました」であるとか、あるいは「労働運動のために労働組合に相談しました」みたいなものについては処罰の対象から除きます、それは正当行為ですという問題意識でございます。

最後、不正競争防止法上の措置として、これは平成 23 年の法改正で導入されたものでございますけれども、憲法上の裁判の公開の原則の、一種、特例措置として、刑事訴訟手続の特例というのが入ってございます。要は、先ほど棚橋会長のお話でもありましたけれども、刑事の法廷の場で営業秘密が漏れてしまうことがあるということについての措置ということでございますけれども、公判における営業秘密を、その営業秘密の中身をそのまま言うのではなくて、記号で呼ぶとか、そういった特別な措置が規定されているということでございます。

その上で、そういう背景事情の下で、ようやく今議論していることについてたどり着いたわけですが、まず議論の経過として申し上げますと、今年の 9 月に産業構造審議会に、営業秘密の小委員会を設置いたしました。その背景として申し上げますと、左側に書かせていただいておりますが、いわゆる成長戦略、日本再興戦略、閣議決定がされたものでございますけれども、日本再興戦略で、営業秘密の漏えい防止対策について、関係する法案を、来年の通常国会という今度始まる通常国会でございませうけれども、関連法案の国会提出を目指すべしという宿題をいただいております。

あるいは、毎年、知的財産戦略本部という、全閣僚と有識者の方々で構成されている会議で決定されている話でございますけれども、知的財産推進計画というものがありますが、そちらでも営業秘密の保護について、法制面についてもきちんとやっていけという宿題をいただいているということで、右側に書かせていただいた小委員会も設置したということになってございます。こちらについては、委員長としては、政策研究大学院大学の後藤先

生という方をお願いしているわけですが、見てのとおり、法曹の方々、学者の方々、産業界、マスコミ、あるいは知財の関係というのは裁判所の代表にも入っていただくのが伝統になってございまして、裁判所の代表として、鈴木判事にお入りいただいているという状況になっております。

その上で、今日、まさに午前中に産業構造審議会で、報告書案についてご審議、ご議論をいただいたということになっているんですけれども、そちらについて、議論の方向性、取りまとめの方向性をご紹介したいと思っております。こちらについて、まだ報告書案でございまして、報告書ではないと。明日か来週早々から、いわゆるパブリックコメントをやらせていただきますので、場合によっては大きく、あるいは小さく変わる可能性もあると。そういう前提で、現段階でのものとしてご紹介させていただくことをお許しいただければと思います。

まず、制度改革については、今回の不正競争防止法の改正をしようと思っているものについては、民事規定の改正のお話と、刑事罰、特に処罰する範囲の話と、先ほど若干申し上げましたけれども、法定刑を引き上げるのかどうかという話の3種類でございます。まず民事の話からご紹介をさせていただきます。

まず1個目が、営業秘密侵害品の譲渡・輸出入の話でございますけれども、分かりやすく申し上げますと、今でも商標権、偽ブランドの侵害物品であります。あるいは特許権の侵害物品なんかについては税関でも輸入が差し止められるように、その譲渡あるいは輸出入なんていうものは不正競争行為として定義される、あるいは特許法違反、商標法違反として定義されるということになってございまして、営業秘密の侵害品についても同様の取り扱いをします。少なくとも、営業秘密を侵害する製品だということが分かっている、それを譲渡する、輸出入するという行為については禁止していくということを考えてございます。

そちらに円グラフを付けさせていただいてございまして、昨年末に私どもが行った調査で、これは私も意外なぐらい高かったんですけれども、わが国企業に対して、営業秘密を侵害している製品というものがどの程度ありますか。経験したことがありますかということをお伺いしたところ、だいたい6割ちょっとぐらいの企業が、営業秘密を侵害している気配がある物品がありますというご回答をいただいているということでございます。

参考のところに書かせていただいておりますけれども、こちらはまだこれから具体的な手続きは検討していくというものでございまして、不正競争防止法に違反すると。営業秘密の侵害物品について、今後、具体的に税関でどうやって止めていくのかと。何よりも問題意識として最大なのは、特許もそうですけれども、営業秘密の侵害物品は外見上わからないですね。偽ブランドのかばんとかであれば、ある程度、外見上分かるというものもあると思っておりますけれども、営業秘密とか、あるいは特許の世界については、何が侵害製品で、何がそうではないのかということは税関の職員には分からないので、どうやって客観的に、公平に、かつ迅速に手続きを進めていくのかということについて、これ

からさらに詰めめの検討を行う必要があるという状況になっています。

右側で、民事規定の改正事項のその 2 で、おそらく実務的にはこちらの方が影響は大きいかもしれませんが、問題意識として申し上げますと、営業秘密の侵害の民事訴訟において、被告が原告の営業秘密を不正に使用しているという証拠というのは、被告側の工場にでも行かない限りは分かりませんと。原告側がその証拠を入手することは難しいですと。立証できませんという議論がございます。実際、そうだと思います。

もちろん、民訴法の文書提出命令を使えばいいじゃないかという話もちろんあるわけですが、当事者の方々なんかにお伺いすると、民訴法の文書提出命令なんかは、まず文書を特定するというのが基本的な前提、原則になり、それこそファイル名とか、そのファイルが存在していること自体を立証することが原則になるんですと。もちろん例外もあるんですけれども、立証することが原則になるという状況の中では、原告が被告の不正使用をきちんと立証するという事はなかなか難しいと。そういう状況の下で、私どもが簡易な調査でやらせていただいたところと言うと、営業秘密の侵害訴訟における勝訴率というのは、だいたい 16% ぐらいしかない。一般的な民事訴訟全体で言うと 8 割弱ぐらいだというのが数字としては把握してございます。もちろん、和解に至るケースとか、和解の内容とかもいろいろで、原告が勝った割合ということだけで単純に良い、悪いということはいえないんですけれども、営業秘密侵害訴訟において原告がなかなか立証することが難しい一つのデータとしてご理解いただければと思います。

ちなみに、民事訴訟のそもそもの訴訟の件数も、日本は非常に少ないです。参考として、韓国と比較させていただきますけれども、営業秘密の関連の民事訴訟として、日本では 13 件の判決が 2012 年にあり、韓国では 60 件余りと。人口の差、あるいは経済規模の差なんかも考えると、日本の訴訟というのは相当少ないと。もちろん訴訟が多ければいいというものでは全然ありませんし、合理的な数字である必要があると思いますけれども、少なくとも、ここまで少ないと、やはり訴訟のシステムに何らかの問題がある、改正の必要性があるということの一つの証拠かなというふうに思っております。

その上で何をやるのかということでございますけれども、ここもなかなか審議会の場では議論が尽きないところであります。ご案内のとおり、民事訴訟法上は、原告が、被告が製造ノウハウ、営業秘密を不正に取得したこと、あるいはその取得した営業秘密を不正に使用しているということを立証しなければいけないわけですが、先ほど申し上げたとおり、不正使用については立証することが相当困難という現実を踏まえまして、今回については、原告は不正取得されたことを立証すれば、被告は使用していないということを、逆に自分が独自技術を使って、その営業秘密で発揮できる性能を出しているんですということを、被告が身の潔白を明らかにしなければいけないという立証責任の転換を行う、原告にとっては立証負担を軽減するという事を考えてございます。

3 点目でございますが、除斥期間。これはやや地味な話かもしれませんが、現行法上は、例えば、営業秘密を盗られて不正に使用されましたと。その場合、差止の期限は、

盗られてから10年に限って差止ができるということになるわけですが、具体的なケースで言うと、新日鉄住金のケースなんかもそうですけれども、かなり長期間がたつてからでないとは分からないんですという経済実態もかなりあるという話はお伺いしますので、こちらについては10年を20年にするということを考えております。

当初は「そもそも撤廃してしまえ」みたいな議論もございましたけれども、先ほどの、立証負担の軽減、被告側に立証責任が転換されますという制度を仮に導入する場合には、日本企業が逆に言いがかり的な訴訟を外国企業から起こされて、被告になるというリスクも考えられなくはないので、そのための文書を保管しておくという期限に限定を付けた方がいいですねということで、20年ということにさせていただいております。

民事は以上でして、今度は刑事の話でございます。まず、ベネッセのケースなんか特に問題意識としてございますけれども、企業情報、営業秘密について、情報通信技術、もっと具体的に言うとスマホの発達、スマホの普及みたいなものはすごく大きいんだと思いますけれども、そういう企業情報というのがいったん漏れるとすぐ拡散してしまうと。しかも、かなり多数の関係者に漏れてしまうという経済実態になりつつあるかなと思ってございますけれども、実際にベネッセのケースなんかで言っても、6次取得者まで行っている、100社以上に漏れていると。そういう状況の中で、ここをどうしていくかということでございます。

現行法は、窃取者、不正に営業秘密を取得した本人からその情報を盗った人だけが処罰対象になるということになってございますけれども、これについて、限定をなくす法改正をやるということを審議会では議論いただいております。ご存じの方も多いかもしれませんが、有体物である盗品、盗まれた品ですね。盗品の譲受罪については、基本的には3次取得者以降も、故意がある限りにおいては処罰しますということになってございますので、それと同等の並びで、無体物である営業秘密についても、もちろん故意があることが前提になりますけれども、2次取得者までに限定せず、3次取得者以降であっても処罰対象にはなり得るという形の法体系にしていきたいということを思っております。

2点目は、先ほど刑事でもご説明したことと全く同じ内容でございますけれども、営業秘密を不正に使用したもの、営業秘密侵害品、特許権侵害物品と同じ並びでございますけれども、営業秘密の侵害品については、民事の方でも差止とかの対象にしますし、刑事罰も科していくということを考えてございます。もちろんのことながら、故意があることは前提ということになります。

3点目でございますが、処罰範囲の拡大の議論として、今、この中にも利用されている方もいらっしゃるかもしれませんが、私もプライベートで利用してはございますけれども、クラウドサービスが相当普及しており、インターネット上に情報を保管する機会が多いと。その場合のサーバーの所在地というのは、基本的には電気代が安かったり、水道代が安かったり、冷やしやすいくところということで、だいたい日本の国外の寒いところ、北の方にあることが多いということをよく聞きますけれども、何が言いたいかと申し上げますと、外国に

保管されていると。物理的に見ると外国に保管されている情報というのが急激に増えつつあると。今、私がこの演台の上でクラウドから情報を引っ張ったとしても、その情報というのは、刑事法的に評価をすると、国外にある情報ですということになってしまって、その取得というものについて処罰対象にならない可能性があるということで、そこについて明確化するというので、国外にあるものであったとしても、国外の取得行為についても処罰対象にするということを考えてございます。

ちなみにでございますけれども、冒頭、棚橋会長からもご紹介がありましたけれども、開示、情報を漏らすこと、あるいはその使用については、現行法でも国外犯として処罰をされる所、今回の法改正によって、取得行為が国外であったとしても処罰の対象にするということでございます。

右側でございますけれども、未遂行為を処罰するという話でございます。こちらについては産業界からもいろいろ議論がございましたけれども、アメリカであっても、日本の刑法はかなりドイツ法を参考をしている部分がございますけれども、ドイツの刑法であっても、あるいは韓国であっても、基本的には、未遂であるとか、いわゆる共謀であるとか、教唆であるとか、そそのかしというものについても処罰対象にしていると。日本でもそうすべきじゃないかという議論がかなり強くございました。私どもとして、結論として申し上げますと、未遂行為についても、審議会での議論としては、処罰対象にする方向で検討すべきじゃないかということでございます。

その最大の問題意識として持っておりますのが、サイバー攻撃なんかも含めた、情報通信技術を使った、あるいは一部使ったような情報の取得行為というものが非常に多くなっている、法益侵害の危険性が高くなっているということでございます。一例として、いわゆる標的型メールを使ったような情報の流出経路をここに書かせていただいておりますけれども、要は、ターゲットの人間関係を事前に調査すると。誰の名義でメールを送れば開封してくれそうかということ調査するということです。その上で、標的型メールを送信しますと。ターゲットになった人が標的型メールを開封する。開封すると、多くの場合は、1回では済まないかもしれませんが、そのシステム、PCなりを乗っ取られると。最後に、外部から情報を自由に盗みとられてしまうという構造になっているかと思っておりますけれども、現行法の中では既遂犯だけなので、④まで行かないと処罰対象にはなりません。一方で、③と④の差というのはおそらくワンクリックしかないですという状況の中で、どこで処罰対象にしますかということだと思っておりますけれども、私どもの評価として言うと、③も④も法益侵害の危険性としてはあまり変わらないじゃないかということで、未遂犯についても基本的には処罰対象にしていくという方向性で詰めの議論をやりたいということを思っております。

その上で、今度は法定刑の議論でございます。先ほど申し上げましたとおり、現行法では自然人に対して懲役は10年、罰金は個人に対して1,000万円、法人重課の場合は3億円ですという刑になっています。それについて、先ほども申し上げたことの繰り返しになっ

てしまいますが、新日鉄住金のケースで言うと、元社員の報酬というのが数億円ですと。賠償も 1,000 億円ですという中で、抑止力として十分なのかと。営業秘密の価値というものはどんどん高まっていますと。あえて権利化を選ばずに営業秘密という形を取る可能性も高いですと。一方で、漏れてしまったら価値がなくなってしまうということを再三申し上げてございますけれども、抑止力が鍵になるという問題意識の下に、どういう形の法定刑をしていくかということでございます。

やや見づらい順番でございますけれども、現行法上の条文の順番ということで理解いただければと思います。まず、懲役あるいは罰金刑、①でございますけれども、こちらについては、懲役刑については基本的には現行の 10 年というものもかなり重い刑なので、十分じゃないかということで、原則の 10 年というところについて変更する必要はないということで、コンセンサスが得られているかなと思っております。一方で、個人の罰金の 1,000 万円というところについては引き上げるということだと思っております。

関連して、④でございますけれども、犯罪収益の没収という議論があります。罰金という形ではなくて、いわゆる収賄とか贈賄の世界では今でもすでにある規定でございますけれども、罰金とは別に、もらった賄賂みたいなものについては全部没収しますということになっているわけでございますけれども、これを刑法だけじゃなくて、不正競争防止法みたいな世界にも移植をして、個人が賄賂をもらって情報を漏らしましたという場合については、その賄賂を全部没収すると。プラスで罰金をかけるということにできないかという議論がございますが、こちらについては引き続き検討することにしていきます。この「引き続き検討」というのは、役所では時々、やらないということの言い換えということがありますけれども、これは真面目な意味での引き続き検討で、いずれにせよ今月中か、あるいは来月中には結論を出したいという意味で、関係省庁と調整中という意味で、「検討」と書かせていただいております。

次は②でございます。海外重課と言っておりますけれども、要はドイツ刑法とか、アメリカとか韓国などで見られるわけでございますけれども、海外で日本企業の営業秘密を使用する、あるいはその使用をするために海外企業に日本企業の営業秘密を漏えいする、あるいはさらに進んで、その前段階として、漏えいするために取得すると。盗み出すという行為について、海外で営業秘密を使用すると、日本の雇用とか経済への悪影響というのが国内の場合よりも高いでしょうという価値評価の下に、海外の場合にはより原則よりも重い刑を科すべきだという議論がかなり強く経済界を中心にございます。こちらについては、一種、階段を設ける。海外で使用する方がより法益の侵害の度合いは高いという議論は、一定の理解はあるんだと思っておりますけれども、こちらについてはまだ結論が得られてないところでございまして、考慮事項として申し上げますと、現行の原則 10 年というものが実はけっこう重いと。

右側に海外の法制の比較表を付けさせていただきます。日本は原則 10 年で、例外はありません。すべてが 10 年ということになっています。アメリカは原則 10 年で、外

国政府に漏らす場合には15年という形になっています。韓国は原則が5年で、外国で使用する場合には10年と。ドイツが原則3年、例外5年ということになってございまして、それと比べても、日本より重いのはアメリカの15年だけなので、それとの比較において、日本をさらに上げることが妥当なのか、刑事法制全体のバランスとして妥当なのかどうか。

さらに進んで、現行の10年というのは、有体物の窃盗罪が10年であるということを一つの大きな参考の材料として10年になっているわけでございますけれども、例外措置を作ることの妥当性なんかも含めて、妥当性を上回るほどの政策的な必要性が、抑止力を高めるといふことの必要性があるかどうかといふことの議論だと思っておりますけれども、こちらについても、単にやらないという意味ではなくて、検討中ということでございます。

③でございますけれども、告訴の要否ということでは現行の不正競争防止法は親告罪、告訴がないと処罰はしないということになってございます。こちらについては、考え方を若干ご紹介させていただいておりますけれども、親告罪とした現行の理由というのは、基本的には刑事裁判において営業秘密が漏えいしてしまうと、かえって営業秘密を盗まれた被害者の被害が拡大してしまうんじゃないかという懸念の下に親告罪となっているところでございますけれども、先ほどの説明と若干重複いたしますが、平成23年の不正競争防止法の改正で、刑事訴訟手続の特例というものができまして、実際に適用実績というのも1件ございますし、近々さらにもう少し出てくるだろうという状況の下では、親告罪のままにしている理由というものが失われているのではないかということが1点です。

2点目は、営業秘密の漏えい、個人情報が出ました、あるいは取引先の企業の情報が漏れました、共同研究の情報が漏れましたという場合に、その被害者と営業秘密の保有者というのは必ずしも一致しないということが2点目でございます。

3点目は、これも特に化学とか、上流の企業からよく聞く話でございますけれども、特に取引先に営業秘密を盗まれましたという場合に、現実には取引のことを考えると告訴なんかできませんというのでもかなりよく聞く議論ではあります。そういうことも踏まえまして、今回は親告罪を基本的には非親告罪とする方向性で議論をしていくということかなと考えてございます。

⑤でございます。先ほど犯罪収益の没収ということで、個人の話をご紹介させていただきましたけれども、個人だけではなくて、要は新日鉄住金とポスコのケースで言うと、新日鉄住金の主張が正しければということがもちろん前提になるわけですが、新日鉄住金の元社員の報酬だけではなくて、その営業秘密を使って実際に稼いだ外国企業についても犯罪収益を没収すべきじゃないかというような議論でございます。

実際にアメリカでも韓国でもドイツでも、犯罪収益は法人であっても没収するということになっているんですけれども、一方で、わが国においては、犯罪というものは自然人がやるものだという建前になってございまして、法人から犯罪収益を没収するというのは先ほどの建前と両立するののかという理論的な整理が必要かと思っております。あるいはその犯罪収益について、盗み取った営業秘密を使ってもうけた収益というものをどうやって正確

に計算するののかといった、実務的に克服すべき課題もあるということで、理論的に詰める時にさらに検討していった、こちらについても、何回も同じことを言って言い訳がましいのですが、単に先延ばしということではなくて、まだもう少し時間がかかるということでございます。

最後、⑥でございますけれども、法人の罰金刑でございます。こちらについても、現行の3億円について引き上げるという方向性を持ってございます。

次のページに、各国比較を付けさせていただいてございますけれども、基本的には日本の法制を今申し上げたみたいな形で、何点か、まだ宙ぶらりんになっている項目もございますけれども、そういうところをやっていくと、少なくともアメリカとか韓国とかドイツとかの法制とほぼ並ぶようなものになっていくのではないかとことを思っております。

あと、この紙には書かせていただいてませんけれども、残っている課題というのが何点かございまして、まず民事の話で申し上げますと、例えば先ほど、立証責任を転換しますと。推定規定を導入しますという話をさせていただきましたけれども、一種、不正に営業秘密を取得したこと、分かりやすい言葉で言うと産業スパイ的な類型に限定して効果が現れるというものでございますので、より広く不正競争防止法の営業秘密に関連する不当行為に対応していくためには、もうちょっと広い射程を持って、それこそ民事訴訟法上の文書提出命令について、何らかの意味で、特則を作っていくとか、その場合にはアメリカのディスカバリーみたいなものも意識していくんだと思っておりますけれども、文書提出命令について、もうちょっと根本的に見直していきますと。

あるいは、国際裁判管轄についてでございますが、外国企業に日本企業の営業秘密が盗まれましたと。外国で盗まれましたというときに、日本の裁判所がどこまでの事件に手を出ることができるんだというような議論については引き続きの検討課題になってございますので、それについては引き続き研究をしていくということになってございますし、その上でということになりますけれども、いろいろな形の営業秘密について、新法を作るべきだと。現行の不正競争防止法というのは、ご覧いただいたように、営業秘密も入っていれば、偽ブランド的なものもありますし、外国の公務員に対する贈賄みたいなものも規制していたりするので、産業界の人の言葉を借りると、混ぜご飯とか、ごった煮とか言われたりすることもあるんですけれども、一種、反省の下に、営業秘密の新法みたいなものを作るべきという議論もございますので、そういうものについても検討をしていかなければいけないということでございます。

あまり残された時間はございませんけれども、残された時間で、営業秘密の管理指針、私どもが平成16年に作らせていただいたものについて、見直しの議論をやってございまして、今日、基本的にはセットされたということでございますので、こちらについてもご紹介させていただきます。

先ほど申し上げましたとおり、不正競争防止法上の営業秘密となるためには、非公知性、

有用性、秘密管理性、その 3 つの要件があつて、それを全部満たせれば初めて営業秘密になって、不正競争防止法上の保護、民事の差止とか予防とか、刑事罰というものが科せられますという構造になっています。

その上で、私どもが平成 16 年に営業秘密管理指針という一種の行政のガイドラインを作っています。これは、別に何らかの法的な根拠があるとか、これに違反するとお仕置きを受けますとか、そういう性格のものではございません。あくまでも、その 3 要件を満たすためには企業としてどういうことをやったらいいですかということを支援するために策定しているものということで、編集の方針としては、当時の判例を分析して、何回か改訂しているうちに、直近のもので言うと 100 個ぐらいの判例、下級審、地裁、高裁のレベルの判例でございますけれども、分析した上で、秘密管理性が肯定的に捉えられた事例、具体的な事例、あるいは否定的に捉えられた事例なんかを編集した上で、裁判所で考慮されるポイントを集めているというものでございます。

その中で、企業からは、現行の指針、あるいはその指針を参考にしているであろう裁判所の実務、あるいはその捜査の実務について、いろいろな批判がございまして、1 つは、指針で書いていることでもありますけれども、あまりに大量の項目、直近の項目では 97 項目で、その中には指紋認証がどうかということも書かれているわけでございますけれども、「いろいろな項目が書かれていて、日本を代表するような大企業であっても、この書かれている項目の半分もできません」みたいなことを言われるとか、あるいは判例について、地裁、高裁の判例であり、まだ最高裁で統一されてないので、一種、当たり前かもしれませんが、混乱がありますと。一部の判例については、「営業秘密の流出とか差止とかに対してあまりに過剰な、鉄壁な保護を求めているんじゃないですか」みたいなことが批判されるとか、あるいは、鉄壁な秘密の管理をしないと営業秘密としての保護を受けられないのであれば、結果として、中小企業なんかはそういうことができないので、研究開発投資が無駄になってしまうのではないですかといったような議論がございました。

その上で、改訂の方向性ということですが、現行の秘密管理性、何を持って秘密管理性があるかということ判断するに当たっては、伝統的に、アクセス制限と客観的認識可能性の 2 項目が必要だという理解がされていますし、私ども経産省としても、そういう説明をしてございました。具体的には、アクセス制限というと、例示でございますけれども、紙媒体なんかであれば、施錠して保管しますとか、あるいは特定の部屋に対して入室を制限しますとか、社内の情報管理規程みたいなところで、こういう情報は秘密ですみたいなことで明確化しますみたいなことを、例えばアクセス制限のところでは、

あるいは、2 つ目のポイントでは認識可能性として、マル秘と表示をしますとか、あるいは社員に対して研修をしますとか、管理体制を整えますとか、ISO を取得しますみたいなことを種々さまざま言われていて、結局、3 要件からするとどこまですればいいんですかというところについて、必ずしもクリアじゃなかったということだと思っております。

その上で、今回の改訂の方向性ということでございますけれども、秘密管理性の要件の趣旨、立法当時の議論、内閣法制局での議論の経過なんかもちろんたどってございまして、外国の考え方、特にドイツの考え方なんか参考にして、手がかりにしながら、審議会の場でいろいろ議論した結果ということでございますけれども、なぜ営業秘密について秘密として管理していなければならないんですかということ、結果として、たどっていくと、その情報に接する社員あるいは取引先、社員等に対して、何が営業秘密かということ、事前を言っておかないと、結果として、その情報に接している社員が後から「実は君が取った情報というのは営業秘密なんだ。けしからん。」みたいなことを言われて、賠償請求をされますとか、あるいは刑事罰を科されますとか、そういう不当な事態を避けるために秘密管理性というのがあるという認識の下に、結論として申し上げますと、特定の情報を企業が秘密として管理したいと。そういう意思を社員が容易に認識できるような状況であれば、認識可能性という言葉で使ってございまして、そういう状況があれば基本的には大丈夫ですということで、先ほどのアクセス制限と客観的認識可能性という言葉で言うと、アクセス制限が手段で、その結果として客観的認識可能性が生まれれば、それで基本的には足りるんですという考え方の整理をさせていただきます。

これについては、パブリックコメントもさせていただきまして、すでに実質的に公開されているので、言って差し支えないかと思っておりますけれども、日弁連とかからもパブリックコメントで意見をいただきまして、こういう基本的なロジックについては、基本的にはご賛同いただいているんだろうということをご理解してございます。

関連する点でございまして、よく実務の世界では、特に大企業の方々からよく言われる話でございまして、特に大企業であれば日本中に支店があります。あるいは、国内外に関連会社があります。業務委託も大量にやっていますという状況の下で、秘密管理性というものをどういうふうに考えるんですかと。同じ情報を共有している場合、どこか1カ所の地点でいい加減な管理をしていけば秘密管理性が認められませんかということになると、その情報について全社的に秘密管理性がなくなっちゃうんですかという懸念がございまして。実際に、具体の訴訟においても、そういう抗弁を被告側がするという事例があるということが背景にあるのかと思います。

それについては、今回の指針でも取り上げて、明示的な議論をさせていただいたわけでございますけれども、基本的には、原則として法人単位で考えればいいんです。委託先とか子会社とかは基本的には関係ありませんということの整理の上で、法人といっても同じ法人格の中で支店があつたり、部門があつたりするところも多いかと思っておりますけれども、事業本部的な一定の営業秘密管理について独立性を持っていると。管理方法であるとか、あるいはその管理方法を守らなかった人に対する臨時的な注意であるとか、一定の独立性を持っているような、そういう単位で判断すればいいんですということで、実務的には、日本企業の場合では、おそらく事業本部であるとか、支店であるとかということが妥当するんだと思っておりますけれども、その単位で秘密管理性が満たされればいいという整理

をさせていただきます。

あと、右側でございますけれども、取引先との関係で、日本企業、担当者によっては、いわゆる NDA、秘密保持契約を結んでいない限りにおいては、取引先との関係で、取引先が自社の営業秘密を不正に取得しました、不正に使用しましたという場合であっても差止とかはできないというような、何となくそういうコンセンサスがあるというような気配もでございますけれども、そちらについても、必ずしも秘密保持契約が大事なのではなくて、基本的には従業員に対するのと同様に、意思を明示しているということがあれば基本的には足りるのではですかと。例えば、秘密保持契約であってももちろんいいですし、確実にと思いますけれども、送付状に「これは当社の営業秘密なので、きちんと管理してください」みたいな感じの言い方であっても、秘密管理意思の明示としては十分じゃないかということ整理をさせていただきます。

最後、諸外国の動向を若干ご紹介させていただきますけれども、先ほど棚橋会長からもご紹介ありましたが、アメリカでは相当問題意識を強く持っていて、さらなる経済スパイ法の強化の議論であるとか、あるいは実務の世界において、企業とアメリカ政府との関係で情報交換するメカニズムを作ろうであるとか、あるいは、伝統的に営業秘密については必ずしも問題意識を持っていなかったであろう EU などでも、統一的な営業秘密の指令案を 2013 年に出して、聞くところでは、「今年の春から夏の間にかけて成立するのではないか」みたいな議論も聞いてございますけれども、EU でも取り組んでいると。韓国でも、先ほど申し上げましたように、かなりの意識で取り組んでいるという状況になってございます。

私の方からは以上でございます。長々とお清聴いただき、どうもありがとうございました。