

営業秘密の論理

— ILC と CB による秘密情報の管理と活用

川上正隆 (株式会社電通法務室業務企画部長)

菊池純一 (青山学院大学法学部・大学院ビジネス法務専攻教授)

The Logic of Trade Secrets: Management and Proactive Use of Confidential Information by ILC and CB

Masataka Kawakami Senior Manager of Business Planning Department Legal Affairs Division, Dentsu Inc.

Prof. Junichi Kikuchi Aoyama Gakuin University College of Law, Graduate School of Business & Law

企業法務には「予防法務」「治療法務」「戦略法務」という3つの役割があり、これまではそれぞれの役割ごとにスペシャリストを養成し、役割ごとの実務対応を行ってきた。

しかし、企業法務がより積極的に独立したビジネス・モデルを指向するのであれば、3つの役割を一元的に運用する「企業法務サイクル」の概念を構築することが望ましい。企業法務を行う者は、ゼネラリストという観点も持ちあわせ、知財のライフサイクルと融合する企業法務と推進する者、いわばリーガル・プロデューサーとなるべきである。

このような観点で営業秘密の保護を考える場合、ILC & CBの論理が必要である。

■キーワード 蜘蛛の糸理論 営業秘密 個人情報 知財アウトカム ILC & CB

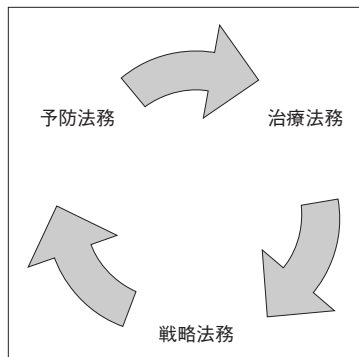
1. 秘密管理の共同体：「蜘蛛の糸論理」

営業秘密でまず適用される法は不正競争防止法であり、ノウハウ、トレードシークレット、ネガティブ情報など、およそ企業として保護したい秘密に対して、「秘密管理性」「有用性」「非公知性」の3要件を課し、法的保護を付与している（不正競争第2条第6項）。さらに、営業秘密の流通形態によって不正競争行為類型を細分化して定義している（不正競争

第2条第2項第4号～第9号）。営業秘密に対してこのように細かく法による保護を付与する理由として、田村（2006）が説明するように、「もちろん、特に法を置かずとも、取締役等に対して競業避止義務が法定されていたり、従業者やライセンシーと秘密保持契約や競業避止契約を締結した場合には、法的な保護を受けることも可能である。しかし、前者については、人的範囲に限定があるほか、取締役の退職後等、基本契約関係の終了後には及ばないとされている。後者の保護も物理的なスパイ行為に対しては無力である。民法709条により対処しようにも、伝統的学説に従う限り、差し止請求を認めることは困難である。そこで設けられたのが、1990年改正により導入された営業秘密（trade secret）の不正利用行為に対する不正競争防止法の規律である」が挙げられる¹⁾。

法の定義する不正競争行為を行った者に対して営業秘密を保有する事業者（保有者）は民事上の損害賠償の請求をすることができ、あるいは、告訴による刑事罰を求めることができる。営業秘密の不正利用がされた企業を被害者として保護する図式であ

図1 企業法務サイクル



り、これは不正競争防止法の法目的（第1条）が、「この法律は、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」という事業者（企業）を保護するという所以による。

しかし、自社の営業秘密に不正行為がなされたという理由をもって、その企業が純然たる被害者として許容されるという社会通念は以下の二つの理由をもって、崩壊し新たな枠組みが登場しつつあるといえる。つまり、自社が信頼して情報を開示・提供した以上、一次開示先、そこからの二次開示先あるいは末端までをも含めて、直接取引がなくても全ての開示元である自社（創成者）が連鎖的に責任を負う、いわゆる、「蜘蛛の糸論理」が社会通念になりつつあるのではないかという仮説である。

従来の社会通念が崩壊した理由の一つは、ビジネス形態の変化にある。企業活動、事業活動の軸は「アウトソーシング：委託業務」「JV：共同事業」が標準になりつつある。自社完結型業務はあり得ないと言ってもよい。したがって、企業活動は共同体ビジネスでありそれは運命共同体にもなり得るのである。特に前者の場合には、委託先選定や管理責任は当然に委託元の企業にある。例えば、予防法務の視点からすれば、委託先に対してNDA等を締結することによる営業秘密の事前予防が可能であるが、戦略法務の視点からは、営業秘密を開示してもよい事業なのか、あるいは当該業務の委託先として適する相手か否かという検討が求められる。「企業は自社の情報セキュリティ管理のみならず、共同研究・開発や売買等の取引関係をおこなうパートナー企業や大学の情報セキュリティ管理についても考慮する必要がある。いかに自社の管理ができていても、パートナーから技術流出するリスクがある」²さらに、委託先で不幸にも営業秘密の不正行為があった場合、治療法務上の視点からは被害者という立場になるが、そもそもそのような委託先を選定した自社にも責任（法的責任はないとしても社会的責任）が存在することになる。

法的な被害者は社会的被害者ではなく、場合によ

っては社会的加害者になり得るのである。つまり、企業の社会的責任からすれば、例え委託先での不正行為としても、企業が免責されることはない、と考えるべきであろう。不正行為の影響が、契約関係を介して、ビジネス網の末端にまで波及することが予見できなかったのであれば、酌量の余地があるが、組織の統括者として知っていたのであれば当然に管理をする義務が（法的にはないとしても）発生する。さらに拡げて考えるならば、それは不正行為の問題にとどまらないということになる。人為的なミスや事故の場合も同様な論理が作用するといえる。持ち出した資料を外に置き忘れた、あるいはPCウイルスなどで流出したというような事故の発生において、委託先以降の第三者が発生場所であったならば、委託元の企業が社会的責任をとらなくても構わないという社会通念上のロジックは存在しない。それは、次に説明する理由に該当する個人情報保護法ではないが、宇治市の住民基本台帳のデータが漏洩した事件の訴訟において、住民基本台帳のデータを委託先から流出された宇治市に対する管理責任を認める判例からも明らかである³。

従来の社会通念が崩壊したもう一つの理由は、デジタル社会の変化である。IT技術の発展により、有体物を扱わない「デジタル商品」のみを取り扱う産業構造「新社会産業型企業」が成長したことである。このような企業では、知財+流通媒体が商品であり企業の生命線である。したがって、情報（営業情報であっても）の取り扱いで間違いを犯す（営業秘密の不正行為をなす）ことは、当該企業そのもの問題であり、当然に責任を負うこととなる。社会問題化しているファイル交換ソフトでの情報流出事故対応をみれば明らかであって、流出した情報を保有している企業は自らを被害者とは説明していない。それが顕著に示されているのが「個人情報の保護に関する法律（個人情報保護法）」である⁴。

不正競争防止法の成立は1934年にさかのぼるが、数次に渡る改正を経ても趣旨は変わっておらず、基本的には先に述べたように事業活動の保護であり、軸は企業の立場であった。他方、個人情報保護法はIT社会での情報の取り扱い、特に弱い立場での個人を守るという観点で2003年に公布された新し

い法律である。護送船団方式といわれる形で企業を守るのではなく、企業にとってのエンドユーザーたる個人を守るという発想に基づいている。そのような立場を貫く企業こそが社会的に守られていくのであり、その思想は法目的（第1条）「この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることにかんがみ、個人情報の適正な取り扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする」に明確に表現されている。

この条文中では、「事業者を保護する」「経済活動を保護する」とは記されておらず、「個人の権利利益の保護」のみが明示されている。そして同法の中では個人情報を取り扱う個人情報取扱事業者の義務として、「第20条：事業者自身の安全管理義務」「第21条：従業員に対する監督義務」「第22条：委託先に対する監督義務」の義務を要求した上で、義務違反の場合は企業に対する行政指導や罰則が適用される。特に経済産業省ガイドラインでは、第22条に関しては事実上末端の委託先までの管理を要求している。つまり、個人情報流出などの事故が発生した場合、例えそれが自社でなく委託先からによるものだとしても、個人情報の保有者たる企業は法的責任が発生するのである⁵。

個人情報とは直ちに営業秘密ではないものの、両者とも「情報」という点は一致している。そして面白いことに不正競争防止法の所轄官庁である経済産業省が上記のようなガイドラインを公表しており、

「企業の保護」ではなく「企業の責任」を求めているのである。

以上の二つの理由により、営業秘密において企業が自らも責任を取る必要性が確認できる。しかしさらに、営業秘密は知的財産の一つであり、企業がその知的財産を使用してビジネスを行うということは、すなわち、特定の知財パッケージによるアウトカムの創出行為でもあると解される⁶。

企業は不正行為が介在した負のアウトカムの創出にならないように責任を持つことは当然のことであろう。正のアウトカム創出のためには、自社における営業秘密の管理のみならず、その営業秘密をビジネスで使用する妥当性を査定し、その知的財産から新たなアウトプットがなされるまでの手法・システムの構築し、委託先などに持ち出す場合のリスクヘッジを解析し、当該ビジネスのライフサイクルにおける内的外的評価を行う必要がある。

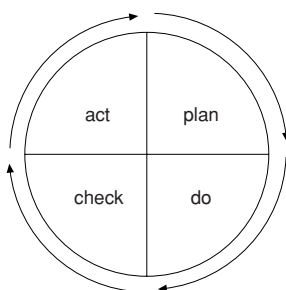
2. 企業におけるマネジメントシステム： 「ILCシステム」

営業秘密のリスクマネジメントは、ISMS（information security management system）に基づくPDCAサイクルによる情報管理が一般的である⁷。

例えば、営業秘密の運用は以下のように扱われる。

- plan : 秘密保持契約 ライセンス契約
- do : 営業秘密を利用したビジネスの実施と活用
- check : ビジネススキームの検証、監査 不正行為の調査
- act : ビジネススキーム、営業秘密保護の改善

図2 PDCAサイクル



- plan …… 目標を設定して、それを実現するためのプロセスを設計（改訂）する
- do …… 計画を実現し、そのパフォーマンスを測定する
- check …… 測定結果を評価し、結果を目標と比較するなど分析を行う
- act …… プロセスの改善・向上に必要となる変更点を明らかにする

Planからdo段階では予防法務として契約等によるリスク回避を行い、doからcheck段階では契約履行の確認や、委託先も含めた監査による検証あるいは事故対応を行う。最後のactでは営業保護体制の見直しや改善、次の業務に向けた委託先選定基準の構築などの治療法務である。さらに蜘蛛の糸論理で委託先の管理責任を免れることが出来ない状況では、委託先との契約(plan)委託先との業務(do)、業務内容の確認(check)、委託業務スキームの改善(act)は事業化において欠かせない戦略法務である。この論理をより一層構造化して統合すると、「統合的法務支援/IILC(integrated legal communication)TM」の展開が可能となる⁸。

そもそもなぜIILCが必要なのか。それは現在の企業においては様々なビジネスがなされており、それに対して法務部門を含め様々な組織、部署、会社が参加しているが、高度に専門化されたビジネスが展開されるにつれそれぞれが分業化、独立化し、組織間、企業間の距離が広がり、明確かつ統一的な情報交換や意思決定、あるいは責任の所在が不明瞭になりがちであり、結果として「総合力」の有効活用がなされない場合が多いためである。ゆえに統合的にビジネスを推進するためのシステム形成が必要となる。

ではなぜIILCの基点を企業法務に求めるのか。それは、まず外的要因からすると、企業活動、ビジネスにはコンプライアンス、法令遵守などが当然に求められ、それをコントロールするのは企業法務に他ならない。内的要因からすると、企業法務サイクルからわかるように、企業法務はビジネスの発生以前の準備段階から実施され、次のビジネスへ展開する全てのビジネスライフサイクルに関係する。このように、企業法務は全体的な俯瞰が可能な機能を持っている。したがって、従来の契約審査や法務相談という分業化した企業サポート的性格から、経営計画の性格に進化することになる。

IILCが提供するものは、企業内で分業化されているビジネスをビジネスライフサイクルに沿って一元的に統合することにより、各業務のシナジー効果を高め、その結果としてアウトカム価値の向上が促進されることに他ならない。経営情報の統合、つま

り、特定の知知的財産の統合によって組織内部にイノベーションが生じるのである。

IILCのシステムは、次の4つの価値モジュールから構成される。

① Relative Communication

主としてビジネスにおける組織的、人的体制のインフラ整備の視点である。例えば、営業秘密を取り扱う規定の整備。組織と人員に対する教育や誓約書などの内部統制。委託先の選定基準やNDA締結などの機能である。内部と外部の両者に対する形式、体制整備によるリスク回避など、基本的な予防法務である。蜘蛛の糸論理で例えるならば、蜘蛛の糸をどこに張り、糸をどのように交差させるかという蜘蛛の巣の作り方であり、すべてのビジネスラインを繊細に関係づけることが求められる。

② Analysis Communication

主としてビジネスサイクルの中での問題点を分析し、例えば営業秘密の流出や漏えいといったトラブルの発生や拡大を未然に防ぐことを目的とする視点である。予防法務と治療法務を兼ね備えた視点であり、Relative Communicationを基礎として展開する位置付けとなる。蜘蛛の糸論理で例えるならば、糸のほつれの修復や巣の強化など、ビジネス全体の弱点を改善し、ビジネスの頑健性向上を図る。

③ Active Communication

主として営業秘密をアウトカム創出のための知財パッケージとして捉え、積極的な活用(ライセンスや新規事業開発)を図る戦略法務の視点である。現在のビジネスのみならず、将来的な成長、発展を目的とする。蜘蛛の糸論理で例えるならば、より多くの巣を張りめぐらして効率的に餌を補足するように、ビジネスチャンスを積極的に拡大することを目的している。

④ Information Communication

ビジネスの各段階での情報を集約し、上記各視点に沿って情報を統合的にコントロールすることで営業秘密を使用したビジネス全体を俯瞰することを目的とする視点であり、IILCのリーガル・プロデューサーには必須の視点である。蜘蛛の糸の論理で例えるならば、張りめぐらした糸の中心にいる蜘蛛が糸上のあらゆる動きを捉えて分析し行動を起こすよう

に、あらゆる情報の収集と分析を行い効果的な意思決定を行うようなものである。この視点がなければ上記①～③は結合せず、独立したものとなり統合化は図れない。

企業法務サイクルとPDCAサイクルを融合させ、四つの価値モジュールを運用することが、企業におけるILCの実践となる。営業秘密の管理に際しては、より一層複合化された知財パッケージ（複数の知的財産が契約ベースや技術ベースなど様々な要素と共に組み合わせられた形態で活用される）を評価管理することが必要になる。

無体物を取り扱う新社会産業型であるコンテンツ産業では、制作サイクルが極端に短いもののコンテンツの二次流通、三次流通という時間軸が加わる。それに附合する知的財産権は主として著作権であり、特許等の産業財産権に比して権利消滅までの時間軸が長い。つまり、企業法務としては、コンテンツの一次流通だけでなく、デジタル複製などの二次流通までも長期に対応する必要が生じる。複数の知財パッケージを統合するピラミッド状のILCモデルが構築される。この場合、流通形態が異なる各々の

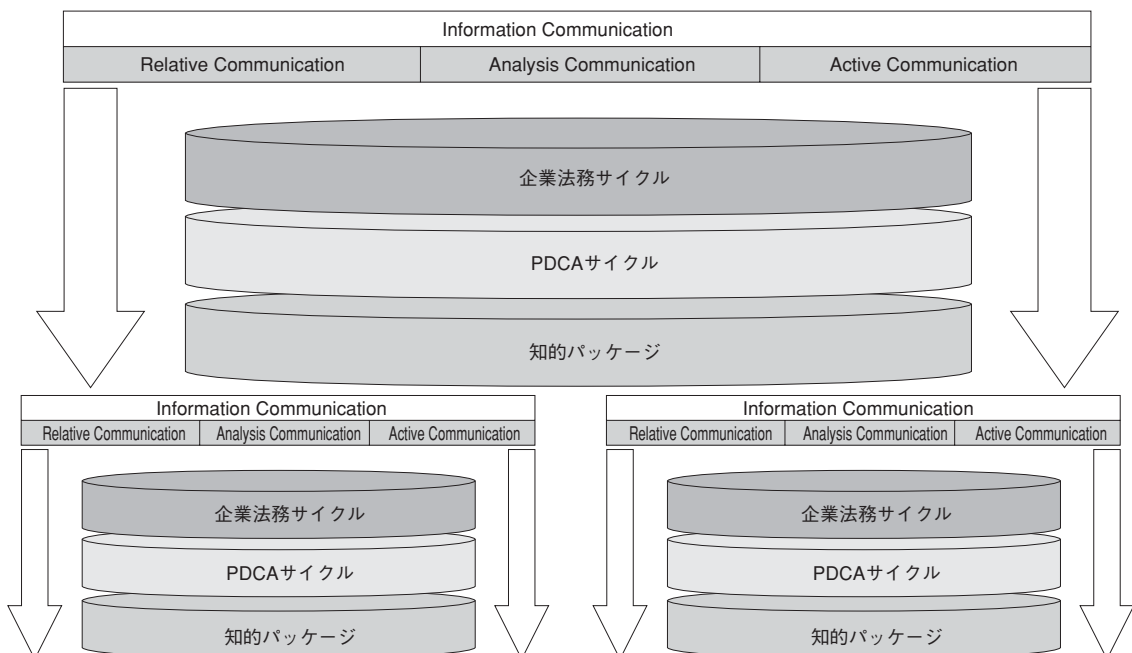
パッケージをさらに統合管理するため、様々な状況で生じるアウトカムをさらに一元化してより価値の高いアウトカムとする必要があるため、パッケージ全体のILCの実践には相当高度なスキルが要求される⁹。

3. 営業秘密の活用化ビジネス： 「Confidential Bank™」

営業秘密は蜘蛛の糸論理により、その責任が財産権者である企業にも帰結するのであれば、企業としては営業秘密を活用したビジネスを控えるべきなのではないか。そのような疑問に直面する。

不正競争防止法では営業秘密を「秘密管理性」「有用性」「非公知性」の3要件で規定している。特に「秘密管理性」「非公知性」の構成要素の基軸で考えるならば、使用しないことが最適な解答となることも考えられる。しかし、「有用性」という要件を加えると、その解答の選択肢が変わってくる。すなわち有用性とは、「当該情報が事業活動に使用・利用されたり、または、使用・利用されることによって費用の節約、経営効率の改善等に役立つことを

図3 ILCの複合化モデル



いう。保有者の主観ではなく、客観的に有用でなければならない」と考えられており、営業秘密でありながら使用・利用を前提とした知的財産であるということになる¹⁰。

そのような「営業秘密」を、インカム・ロジックに基づいて組織内部に死蔵してしまうのではなく、アウトカム・ロジックに基づき、新たなビジネス・モデルを付加することも選択肢である。例えば、ILCシステムにおける active communication の視点から営業秘密を積極的に展開しつつリスクヘッジを行うにはどうすべきか。

そこで、一つの選択肢として、「Confidential Bank (CB)」ビジネスを提案する。これは企業における営業情報を Confidential Bank (CB) にエスクロー（預託）して活用するビジネスである。知財でエスクローは聞きなれないかもしれないが、コンピュータ・プログラムのライセンサーの財務状況に不安がある場合、リスク回避の一つの手段として、「コンピュータ・プログラム・エスクロー」の制度がある¹¹。

スキーム案としては、

- (1) 極めて高度のセキュリティレベルを保持するCBを立ち上げる。

社会通念上からみて、営業秘密を保管（アナログ的にもデジタル的にも）するのに相応しいほどの高度なセキュリティレベルが求められる。

- (2) 企業はエスクロー契約を行い、CBに営業秘密を預託する。

通常の機密保持契約ではなく、エスクロー契約とすることで、企業間取引の安全性を保証することも

目的である。

- (3) CB側では、営業秘密の3要件を評価する。

CBとして高度なセキュリティで管理するため「秘密管理性」は充足しているがそれに加えて、「有用性の評価」、「非公知性の確認」を客観的に行う。

- (4) 企業の依頼により、当該企業の委託先や共同事業者の情報管理の評価を行う

秘密情報の開示先の評価を行うことで、情報開示のリスク評価が可能となる。

- (5) (4)の評価に適合した所に営業秘密の引き渡しや回収などの運用を行う。

情報の移動についても安全性の保証を担保することができる。

- (6) CBは営業秘密の管理、運用に伴う知財基金をビジネスとする。

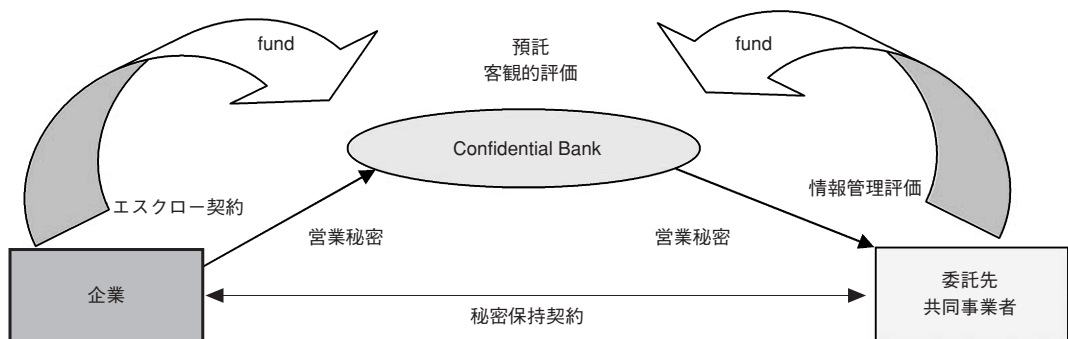
CB自体が独立事業体として存在し得るために必要である。

というのが、CBビジネスのスキームである。もちろん、これらのスキームは前述のILCによって統合的に展開しなければならない。

CB自体が営業秘密を直接に管理するため、情報管理、セキュリティレベルについては相当に高度なものが要求されるが、現実的に「重要情報保管庫サービス」のようなビジネスは出現しており、このサービスに「評価というコンサルティング機能」「fundの機能」を付加すれば十分に存在が可能であると思われる。

営業秘密の保有者である企業側のメリットとして、営業秘密の3要件の客観的な充足化が挙げられる。なぜならば、企業にとっては「秘密管理性」

図4 CBのビジネススキーム概念図



「有用性」「非公知性」を客観的に自証することは難しいからである。本来営業秘密として厳重に管理すればするほど、どのように管理していたのかという管理性はそれ自体が企業秘密に該当するため、明確にすることはできない。また、有用性というのは第三者との関係で比較考量するものであり、内部のみの判断では客観的な有用性は計れないからである。非公知性については、公知であるか否かは第三者が評価する客観的視点であり、そもそも公知であれば企業は営業秘密として保有する必要性がない。このような客観的評価を行うことで、後々にこれが保護に値する営業秘密やノウハウだったのかという係争が生じることも予防可能となる¹²。

これらの要素を客観的にCBで判断することにより、主観的に企業が考えていた営業秘密自体の客観的な価値創造が可能となる。すると、ライセンスなどの事業では、ビジネスのための価値評価が可能となるうえ、知的資産会計にも適用できることにもなる。CBの評価により従来よりも積極的なビジネス展開を発展できるかもしれない。また、CBが委託先などの情報管理評価を行うことにより、外部に営業秘密を渡す場合のリスクヘッジを行うこともできる。

企業から営業秘密を託される者（受託者や共同事業者）にとってもCBが介在することで大きなメリットが生じる。それは、不正競争防止法第19条「第3条から第15条まで、第21条（第1項第11号に係る部分を除く。）及び第22条の規定は、次の各号に掲げる不正競争の区分に応じて当該各号に定める行為については、適用しない。」という規定から生じる。この条文は「本号は、営業秘密を善意・無重過失で取得した場合には、当該営業秘密に関して契約等に基づき取得した権限の範囲内で、当該営業秘密を使用又は開示できることとするものである。」との趣旨であり、社会通念上妥当な方法・目的で営業秘密を入手した者は、例えそこに不正行為が介在したものであったとしても、善意・無重過失ならば当初の方法・目的の範囲内での使用を認めたものである¹³。

営業秘密を受理する側に立てば、そこに不正行為が介在していない確認・証明を保有者に求めること

は、立場などの関係上（大企業と中小の委託先など）から難しい場合が多い。保有者もまた自証することが難しいことは先に説明したが、それならば、蜘蛛の糸論理で連結している当事者がそこで取り扱うものについて不確定な状態であることは好ましくない。そこで、CBに預託し、客観的評価をしたCBから正当に受理することで、不正競争19条1項6号の要件を満たし、安定した取引関係を行うことが可能となる。

CBの活用はこれだけではない。CBが銀行である以上、営業秘密そのものを知財派生の商品として様々に活用することが考えられる。一つは、営業秘密を利用したビジネスについてCBがファイナンスを行うことである。企業がビジネスをCBに信託し、CBが投資家、ライセンシーのビジネスフレームを構築する。投資家、ライセンシーからすれば、CBが介在することにより、営業秘密の内容がわからないとしても客観的に評価されているという実績、信頼性をもとに資金投資をすることができる。営業秘密の保有者である企業は、CBが評価した価値評価の範囲内でビジネスを行うことでリスクヘッジができる。

また、企業として利用価値を見出せない営業秘密、使用予定のない営業秘密をCBがコーディネートを行い、知的財産の流通ビジネスを構築することで、営業秘密に新しい価値を創造することも考えられる。

今後、ILCシステムにCBモデルを組み込むことによって、営業秘密の資産ビジネス・モデルを構築することが望まれる。そのための理論構成を具体的にまとめ、そのモデル実験を実施し、ILCシステムの有用性を検証することを予定している。

-
- 1 田村善之（2006）『知的財産法（第4版）』有斐閣、pp.35-36。
 - 2 一色正彦（2005）『技術流防止のための企業戦略』永田晃也・隅蔵康一責任編集『MOT知的財産と技術経営』丸善、p.158。
 - 3 最高裁「宇治市住民基本台帳漏洩事件」2002年7月11日決定。
 - 4 吉川達夫・森下賢樹・飯田浩司編著（2004）『知的財産のビジネス・トラブル』中央経済社、pp.97-101。
 - 5 経済産業省（2004）「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」10月。
 - 6 Kikuchi, J. (2005) "Outcome Management of Intellectual Assets," *International Journal of Intellectual Property, Law, Economy and Management*, 1, pp.47-51.
 - 7 財団法人電力中央研究所編『知的財産報告書』平成18年8月では、研究開発成果のアウトカム・マネジメントが報告されている。
 - 8 岡野靖文（2006）「営業秘密に関する情報セキュリティ管理」『知的資

産創造』5月号では、組織対応を始めとして、ステークホルダーの管理体制が必要であるとしている。

- 9 末吉互（2005）「高度戦略的知財活用」『NBL』1月号においても、知財の高度戦略化における人材養成の必要性を課題としている。
- 10 青山紘一（2006）『不正競争防止法（第3版）』法学書院，p.81。
- 11 経営法友会法務ガイドブック等作成委員会編（2003）『知的財産法務

ガイドブック』商事法務，pp.129-130。

- 12 大阪高裁「ポリエチレン製法事件」1996年12月26日判決での争点の一つ。
 - 13 経済産業省知的財産政策室編著（2006）『逐条解説不正競争防止法平成16・17年改正版』有斐閣，p.157。
-