

## 企業の技術管理と技術流出

大 野 茂\*

**抄 録** 技術を柱に事業を営む企業にとって技術管理は、経営の要である。然るに、最近、特許出願の公開を介して、或いは人的キャリアーやインターネットを介した外部不正アクセスによって、自社の技術が外部に流出し第三者がいつの間にか使用している、或いは技術動向が分析されているといった事態が少なからず発生している。各企業は、技術流出防止を如何にするか躍起になっているが、特許権という排他的独占権は事業戦略上重要な経営資源であるし、出願すれば公開されて自社の重要技術或いはキー技術が競合相手に流出してしまう、といったジレンマに陥っている。

本稿では、企業における技術管理はどうあるべきか、技術流出をどう捉えどう防止するのか、事業優位性の確保・維持による競争力強化の視点で検討し概括してみる。

### 目 次

1. はじめに
2. 企業における技術情報管理
  2. 1 特許制度と技術情報管理
  2. 2 キヤノンにおける技術の保護管理
  2. 3 技術流出防止対策
3. 中国における営業秘密
  3. 1 中国の営業秘密の要件と労働者対策
  3. 2 日本の不正競争防止法での中国における営業秘密侵害対策
4. あとがき

### 1. はじめに

最近、頓に、製造業における意図しない技術流出（以後、「技術流出」は、断りない場合は意図しない技術流出の意味で使用する）が問題視されている。しかし、技術流出は、今に始まった訳ではなく昔から存在していた。昔と今との違いといえば、日本の企業の立場が変わったこと位である。欧米企業に追いつけ追い越せの時代は、技術流出元は欧米企業であり、技術流出先が日本企業であった。その後、日本の企業

が先進国並みになると、技術流出元が日本の企業になり技術流出先がアジア諸国の企業、特に韓国・中国の企業になっている。米国が、嘗て、官民を挙げて「技術タダ乗り論」で日本を攻撃して来たのは、日本企業に技術が流出して日本が世界の生産基地化し、その立場を日本が奪うことで米国の国際競争力が低下するという国家的危機感からであった。当時の日本の企業は皆、特許情報・学術論文等の公開情報をはじめとして手段を選ばず手当たり次第に技術情報を収集・分析して米国企業の技術、特に生産技術を習得し、その習得した生産技術を限界まで高める改良を行って国際競争力を高めた。その結果、日本は、世界の生産基地として確固とした立場を築き、その後の経済発展と繁栄が齎された。「JAPAN AS No.1」と騒がれていた時代である。

しかし、やがて、日本企業同士の生産コスト

\* 東北大学 未来科学技術共同研究センター 未来情報産業創製寄付研究部門 知的財産・法務統轄担当工学博士（キヤノン株式会社 知的財産法務本部長、副本部長を歴任） Shigeru OHNO

## 本文の複製、転載、改変、再配布を禁止します。

の競争が始まり、日本の各企業は、日本での慣習のままの技術管理下で競ってレーバークストの低いアジア諸国に生産工場を移す戦略に転化するようになった。現地での生産規模が増大するにつれ現地工場からの技術流出が起こるようになって暫くすると競合する現地企業が現れ始め、日本企業を圧迫するようになった。日本の企業が、アジア諸国、特に、タイ、ベトナム、中国等に工場を移して生産競争力を増すまでは良かったが、その後、其の立場を現地企業に奪われ競争力を急速に失うようになっていった。その結果、中国が世界の生産基地となり、日本は生産基地の空洞化を招いた。将に今の日本は、当時の米国と同様の立場におかれている。

しかし、今の日本が当時の米国と違うのは、意図しない技術流出が日本の企業の競争力を失わせ、ひいては日本産業の将来がない、技術流出防止が大事だ、技術を流出させるな、等と国を挙げて大騒ぎしているに過ぎない点にある。

当時の米国は、日本が世界の生産基地化していく過程で、米国が力を維持、或いは力をつけなければならない技術分野は何か、日本の強いところはどこか、を冷静に分析し基礎科学の研究から実用化技術の開発まで官民学が一致して対処することにより今日の米国企業の優位性を築いた。

今や日本も、技術流出防止一点張りではなく、国際競争に強い日本の産業を育成するために何をすべきか、政産学官の智慧を結集しなければならない時期にきている。将来の市場を支配する高付加価値製品とはどのようなものか、競争力を継続的に維持するにはどのような新しい技術が必要なのか、レーバークストに依存しない生産技術とはどのようなものでどう開発すればよいのか、開発した新しい技術をどう守ればよいのか、産業戦略を政産学官一体となって考えその実践に邁進する必要がある。

ビジネスが競争という土俵で展開される以上、競争相手の優れた技術を手に入れて競争力を増強するのは企業が生き残るための手段の一つである。実際、例えば、合法的なM&Aやリバースエンジニアリングによって技術が流出することは避けられない。この場合、合法的とはいえ、意図しない技術流出に相当する場合は多いのは周知のことである。

又、電子化、デジタル化により技術情報の管理がし易くなった一方で、ネットワーク・インターネットの発展につれて技術情報が流出する機会も増えている。

しかも、セキュリティの如何によっては、メモリー技術、圧縮技術、通信技術の進歩も手伝って、大量の技術情報がしかも再利用の容易な形態でネットワークを通じて瞬時に流出する可能性は否めない。

技術情報は一旦流出すると、流出先が特定できても流出技術が流出先で人的に蓄積されているので完全に取り戻すことは実質的に不可能である。覆水盆に返らずの譬えそのもので、精々、流出先に完全な使用禁止を課し、犯した場合は損害賠償請求権を行使するのが関の山である。又、監査権を得て機密管理をさせるとしても、二次流出の防止は難しい。

特に、ノウハウ（以下、KH）の対象とすることの多い、完成品や部品、材料等に化体しない製造技術は、相手製品が自分の技術を使用して製造されたのかどうかを製品自体からでは確認しようもない。若し仮に同じ技術だと確認できたとしても、その技術がこちらから流出したものであることを立証するのは極めて困難である。

技術に限らず、先進国から新興国に情報が流れるのは水が高いから低きに流れるのと同様で避けられないことである。情報は、先進国から新興国に流れるから価値を生む。今日のようにサイバースペースの社会であれば、CIS（cyber

本文の複製、転載、改変、再配布を禁止します。

information supplier) が必要な情報を何時でも提供してくれる。今や、サイバーアタッカー等による技術情報の不正入手とその売買市場の存在が流出技術の売買ビジネスを盛んにしている。

情報社会といわれて久しいが、ネットに繋がっている限り情報は何時でも盗まれ得る状態にある。技術流出も情報漏洩の一種であるが、情報漏洩となると、何も政府や官公庁の場合だけではなく、企業においても不正アクセスや内部犯行などによって日常茶飯事に起きている。企業における情報漏洩が目立たないのは、漏洩が企業の私的事項であり、余程の技術でない限りニュース性に乏しいからである。

しかし、技術流出のもっと深刻な今日の問題は、単に技術が流出するだけに留まらず、その技術の専門家・熟練者が技術の指導者・移植者として流出することである。人的キャリアーによる技術情報の流出である。60歳定年と再雇用環境の悪化は、長寿化が進む中で、人的キャリアーによる技術情報の流出を加速している。新興企業にとっては、技術の専門家・熟練者の確保は、技術開発投資の効率と開発期間の短縮、若手人材への技術移植の点で競争力を増すことが出来るので魅力的である。中国や韓国の企業は、3年間で1億円から2億円、技術分野によっては衣食住の一切を提供して3年間で数億円支払って雇用する場合もあるという。数年前大量に定年を迎えた団塊の世代が、これらの企業のターゲットになっている。

日本企業が米国企業から生産技術を習得していた時代には、人材の流出は、ヘッドハンティングということはあったにしろ殆どが学問の世界のことで、実業の世界では希なことであった。今の時代は、人材を獲得することで技術の習得と開発期間の短縮を図るのが企業戦略の常識になりつつある。

将に、今は、人材も含めた技術情報の管理の巧拙が企業の生き残りを左右する時代になっている。

## 2. 企業における技術情報管理

### 2.1 特許制度と技術情報管理

製造業にとって、競合他社より魅力的な商品を市場に出し続けるために継続的に技術開発することは事業戦略上重要なことである。企業である以上、開発した技術は、競争優位を維持するために、意図しないで競合に真似された場合に権利侵害で訴えられるように法的に保護される。開発した或いは第三者から正当に取得した技術の中で、製品等に化体し製品を観察或いは分析・測定・計測するなどすれば明らかになる技術の場合は、特許権や実用新案権（以後、断りなく使用する「特許権」は、実用新案権も含む意味である）で守り、そうでない技術は、KHのように秘匿状態（ブラックボックス化）にして守るのが一般的な知的財産戦略である。秘匿状態にして守る技術の中には、特許性の希薄な技術や公知の技術も含まれる。これらのことは、今日でも基本的には変わらない。

しかし、現在の世界の特許制度は、図1に示されるように、①公開主義、②属地主義、③最大権利存続期間20年、という制約を有している。

世界の特許制度は、

- ①出願公開主義(出願内容の世界同時公開)
- ②属地主義(特許権は国毎に独立に成立)
- ③権利存続期間は最大20年が原則

を前提にしている為に、次のリスクが生ずる。

- ①⇒不出願国への技術流出に繋がる。研究・開発動向が分析される。ただ乗りされる
- ②⇒①のリスク回避には多数国への出願が必要(多大な特許費用)
- ③⇒権利満了による参入障壁の消失

図1 技術保護管理の前提

## 本文の複製、転載、改変、再配布を禁止します。

その制約から、ネット社会の特性である情報公開の世界同時性のリスク、企業活動のグローバル化の進展に伴う市場のボーダーレス化による知財費用の増加と人材不足からのリスク、及び権利満了による参入障壁の脆弱化のリスク、が生じている。

日本の特許法に公開制度が導入された時代は、日本で公開された特許情報を他の国から閲覧するのは実質上難しかったし、公開された特許情報を他の国の不特定多数の人に同時性をもって配信するのも難しかった。属地主義と公開制度の趣旨が整合していた時代である。

しかし、インターネットの時代は、ネット上に公開した情報は、どこの国でも、誰でも同時に閲覧できる、世界同時公開性の時代である。世界同時公開性になると、発明技術の公開の代償に特許権という独占権を得て発明技術を守るには、特許制度の属地主義との関係で世界中の国に出願していなければならず、膨大な費用が掛る。出願していない国があれば、公開された発明技術は、その国では、自由技術となり誰でも実施できることになる。属地主義と世界同時公開性の矛盾である。

製品を製造する企業にとっては、これまで述べてきたことを前提として、特許権で保護すべき技術（発明）と機密管理下で保護すべき技術（発明）とを、発明が生まれた当初より明確に区別して技術管理する戦略の下に事業を行うことが肝心である。

## 2.2 キヤノンにおける技術の保護管理

キヤノンでの技術の保護管理は、図2に示す体系で行われている。

キヤノンが所有する技術（発明）は、法的に保護する（法的保護）技術（発明）と法に頼らないで保護する（非法的保護）技術（発明）とに大別される。法的保護の対象に分別された技

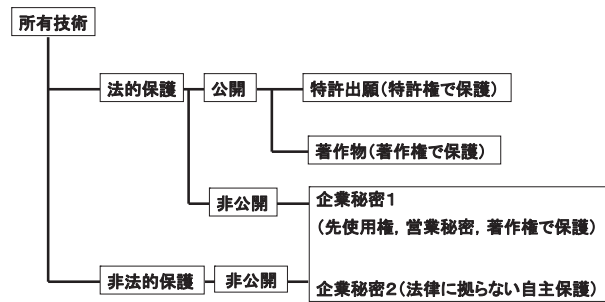


図2 技術保護対策体系

術は、公開の是非について技術・事業・知財の3視点から検討される。公開の是非の決定は、知財の管理職と開発の管理職との合意に拠ってなされ、発明者は対象の発明（技術）を客観的に説明する説明役を担当する。非公開とされた技術は、企業秘密1として社内の機密管理体制下で管理される。企業秘密1とされた技術は、その特性や特徴、実施される大凡の時期、適用分野等を検討し、営業秘密として管理するのか、先使用权を確保するのか、著作権で保護するのか、を決める。

非法的保護とされた技術は、企業秘密2として管理される。

企業秘密1、企業秘密2とされた技術は、公開しても良い時期が来た折には、競合等に公開すると悟られないように（企業秘密にあったことが知られないように）公開する。先使用权は、他社出願リスク回避のために確保するものであるが、後述するように、先使用权制度を設けている国が少なく、その権利幅も決して広くない、寧ろ狭い国もある、要件成立のための準備と管理に大きな負荷が掛る、など、決して使い勝手の良いものではない。キヤノンでも余程の技術でない限り先使用权の確保に動くことはない。

キヤノンでは、技術流出防止に重きを置く技術か特許出願に重きを置く技術かは、図3に示す考え方に依る。

検証可能で特許権行使する技術は、特許権に

### 自社技術保護の考え方

- 1.【検証可能で権利行使する】技術 ⇨ 出願  
-参入障壁構築型-
- ・ビジネスに必要な国で特許権を確保する
  - ・必要によっては、権利行使を行い 事業、技術を守る
- 2.【権利行使不可/しない(KH等)】技術 ⇨ 非公開  
-ブラックボックス化型-
- ・たとえ、製品が徹底的に分析されても技術が知れない
  - ・推測できない
  - ・先使用权確保による他社出願リスクの回避

図3 技術流出防止と特許出願

よる参入障壁を構築するために原則出願する。出願しない国（非出願国）に技術が流出し非出願国で他社が製品に実施したとしても、事業上それ程問題がない技術である。このような技術には、例えば、主要国で特許権を取得すれば事業の優位性が決まる技術が挙げられる。勿論、大事な技術は、将来投資の視点から主要国に限らずに出願し、出願国の数を充分多くする。

市場に出す製品を徹底的に分析されても推測すら出来ず実施若しくは痕跡が知れない技術、つまり、流出して他社が実施しても検証不可か検証不可の可能性が高い技術、或いは新規性のない技術や特許成立の可能性がないか可能性が極めて低い技術で有効性の高い技術は、企業秘密の管理下で保護する（ブラックボックス化型の技術）。その中でも特許成立の可能性がある技術は、他社の特許出願リスク回避のために実施国の想定の上で先使用权の取得の準備を適宜行うようにしている。

## 2. 3 技術流出防止対策

### 2. 3. 1 技術流出防止対策関係の指針等

技術流出防止の指針若しくは対策を立てる際に参考にすべき資料としては、①「技術流出防止指針～意図せざる技術流出の防止のために～」<sup>1)</sup> および「その関連参考資料」<sup>2)</sup>、②「営業秘密管理指針」<sup>3)</sup>がある。

情報セキュリティ関連では、③「情報セキュリティポリシーに関するガイドライン」<sup>4)</sup>、④「情報セキュリティ管理基準」<sup>5)</sup>がある。

情報システム関連では、⑤「情報システム安全対策基準」<sup>6)</sup>、⑥「コンピュータウイルス対策基準」<sup>7)</sup>、⑦「コンピュータ不正アクセス対策基準」<sup>8)</sup>、⑧「情報システム安全対策指針」<sup>9)</sup>がある。

これらの指針、ガイドライン、基準等は、現行の自社の技術流出防止対策の見直しをしたりする場合や、今後新たに技術流出防止対策を講ずる場合は、自社の専門部署の者に一通り読ませておくのが良い。

### 2. 3. 2 技術流出防止対策の基本事項

KHなど秘匿技術情報の流出による影響は、時には企業にとって大打撃になる。例えば、同業他社に技術が流出したら、特許取得されて製造差止・事業中止を招くか、或いは競合品が生産されて市場・顧客の喪失を招く恐れがある。

従って、技術流出防止対策を立てる際に、考慮すべき基本的事項を外さないことが肝要である。

考慮すべき基本的事項としては、先ず、流出防止の対象とする技術を選択する会社基準を策定することである。次いで、策定した基準に従って流出防止の対象技術を選択する。選択の際は、何故、流出防止をする必要があるのか、流出すると事業にどのような影響を与え、その損害はどの程度が見込まれるのか、代替技術はあるのか、あるならその優劣はどうなのか、等々、出来るだけ客観的に分析し、どのような流出防止対策をどの程度の確固さで設ければよいのかの見通しを付ける。①重要な技術情報の特定と流出防止対策の見通しである。

次に、②自社、関係子会社、協力会社、委託会社、ライセンサー等の情報管理体制の整備を行い、③情報管理体制のための専門部署を設置

## 本文の複製、転載、改変、再配布を禁止します。

するとともに、④人事労務管理体制の整備も行う。

管理体制下で仕事する者や該仕事する者と仕事上の接触がある者等と、⑤秘密保持契約等の締結をしておく。⑥関係子会社、協力会社、委託会社、ライセンサー等に対する継続的監視や、⑦実施する国の法規制及び判例等の動向監視を怠らないようにする。⑧技術流出防止対策を最大限講ずる姿勢を従業員全員に常時示し、経営トップ層だけでなく従業員全員の意識向上を図る。

アジア諸国で技術流出防止対策を実施する場合は、企業イメージを良好に保って「現地企業」として認知されるために、企業PR活動、CSR活動、現地人材の育成、地域社会貢献、環境保護などあらゆる手段を講ずることも必要である。

技術流出防止管理策の実施の良否には、円滑な管理が出来る組織と適切な人材配置が大事であり、日常の管理においてPDCAサイクル<sup>10)</sup>を確実に実施し、特にC（監査、評価）、A（見直し改善）に注力することである。

### 2. 3. 3 技術流出の媒体と流出先

一般的に、技術KHが含まれるものの例としては、製法、製造条件、製造装置、図面、金型、データ、構造、原材料、中間体、製造工場、製造設備、外注先情報、共同開発・共同生産等の共同相手情報、等々が挙げられる。

流出媒体としては、「人」と「もの」とに大別される。

「人」としては、従業員、派遣社員、顧客、外注先、設備メンテナンス、コンサルタント、共同開発・共同生産等の共同相手先や協力会社の従業員・派遣社員・顧客、等々が挙げられる。

「もの」としては、情報システム、電子データ、サンプル、図面、金型、文書、資料、写真、カタログ、研究レポート、研究ノート、技術打ち合わせメモ、等々が挙げられる。

「流出先」は、大概、競合企業、顧客企業、仕入先企業、委託先企業、共同開発企業、共同生産企業、等である。

### 2. 3. 4 KH等の技術情報の流出防止策

技術情報の流出媒体が、「人」と「もの」であるから、これらを厳重な流出防止管理体制下に置く必要がある。

「人」の場合は、自社の社員等の従業員に対しては、誓約書、労働契約、就業規則、競業禁止義務契約等の人事労務管理契約を締結し、教育や啓発によって自覚を促すことや適切な処遇により愛社精神を養成する。顧客に対しては、機密保持契約を締結したり、見学を禁止したりする。仕入先や委託先とは、機密保持契約や技術供与契約を締結する。

「もの」の場合は、情報管理体制を設置したり規定を設けたりして、情報管理を厳格に行う。

情報管理のツールである情報システムに対しては、アクセス制限を設けることや認証トレーサビリティを行うようにする。電子データは、暗号化し、持ち出し制限（人、場所、時間）も掛け、必ず記録を残すようにする。文書・資料に対しても持ち出し制限（人、場所、時間）を掛け、必ず記録するようにする。

サンプル・写真・カタログの提供制限とその記録は必ず行い、研究レポートも発表制限し、記録を残すようにする。

### 2. 3. 5 キヤノンの事例

キヤノンのアジアへの工場進出は、1980年代と極めて早い。当時から、日本的経営の良さを前面に出して工場を稼働させていた。ところが、2000年代初頭頃になって、技術流出が話題になり、改めて海外の生産会社における情報の管理状態を確認したところ、日本での情報の取り扱いと変わらない状況であった。特に、技術情報の取り扱いは、例えば、図面等、関係者皆

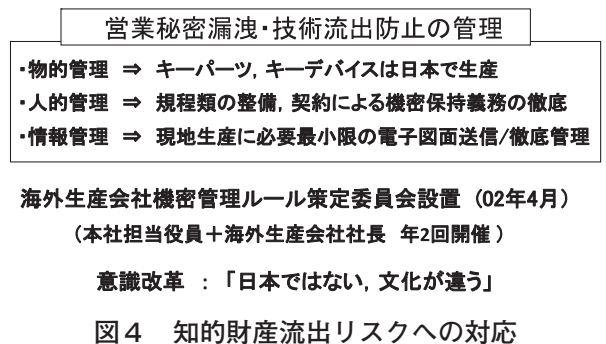
**本文の複製、転載、改変、再配布を禁止します。**

で閲覧し検討する、キーデバイスの技術情報を無制限に現地に送る、部品調達のKHや営業秘密事項を現地の部品調達部門の略全員が知っている、等々、凡そ機密管理とはいえない状況であった。

懸る状況を打破すべく検討委員会を設置し、関係会社も含め技術情報の管理体制の確立を急いだ。

今のキヤノンにおいては、技術情報に限らず、経営KHも含めて知的財産と捉え、知的財産の流出リスクに関する対応体制を確立している。この体制整備は、親会社に限らずグループ会社にも徹底させている。特に、日本にある会社は、技術情報の管理に比較的甘い感覚があるので、親会社の担当部門が、機会あるごとに、グループ経営トップに再認識させている。特に、経営トップの交代の時は、新たな経営トップに認識して貰う機会を設けて改めて自身の会社の知的財産流出防止体制のチェックと見直しをしてもらうことにしている。

キヤノン（グループ）における知的財産流出リスクへの対応の基本的考えが、図4に示されている。



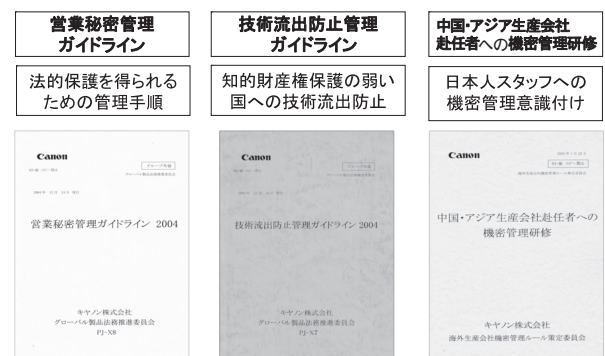
管理対象は、「もの」、「人」、「情報」の3つに分類してある。  
「もの」として一番大事なものは、自社完成品（製品）のキー部品又はキーデバイスである。これらは、日本で自社生産され、海外に輸出される。飽く迄も厳重に管理されて日本で、日本人によ

り生産される。キー部品又はキーデバイスに使用される又は使用されているキー技術、及びそれらを生産する際に使用されるキー技術は、営業秘密管理対象とされ、前述した技術流出防止対策が施されている。これらのキー技術の中には、先使用权の確保を目的として、先使用权要件を満たすように、必要な書類と物、データ等の証拠類の準備と然るべき法的手続きがされて厳重に保管されている。証拠類は、地震、火事等の災害の対策のために、同じものを2ヶ所に分散して保管している。

「人」に対しても、前述の人に対する技術流出防止対策が施されている。例えば、規定類の整備や契約による機密保持義務付けの徹底を図っている。教育・研修・指導は、部門別、世代別、役職階層別、入社年度別、等、木目細かく定期・不定期を問わず、繰り返し行っている。関係会社に対しては、親会社の専門部門の下級管理者や担当者が、時には上級管理者自らが関係会社に出向いて教育・研修・指導を行う。

海外は、「日本ではない、文化が違う!」「日本方式は通用しない!!」と徹底的に意識改革を図るようにしている。

2002年4月からは、親会社担当役員と海外生産会社社長を対象に、海外生産会社機密管理ルール策定委員会を設置して、年2回開催し、海外生産会社機密管理ルールを策定した。ガイドラインや研修冊子も作成し（図5参照）全従業



**図5 ガイドライン等の策定・運用**

## 本文の複製、転載、改変、再配布を禁止します。

員に配布して、関係会社も含めて説明会を実施した。

これらは、修正・加筆が生じると即座に対応し改訂版を出す様に組織としてルーチン化されている。

### 2. 3. 6 非出願対象技術（秘匿技術）の仕分け

出願し公開されることで、技術が流出するので、技術を社内に秘匿することで流出防止するには、技術KH等、技術流出を防止する技術（発明）（非出願対象技術）と出願する技術（発明）（出願対象技術）とを仕分ける基準を設ける必要がある。

図6に、その一例が示される。

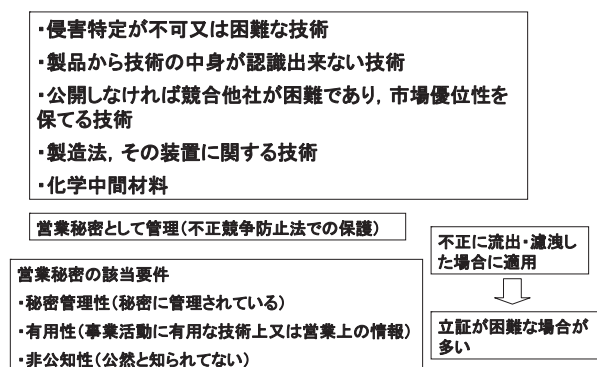


図6 非出願対象技術（秘匿技術）

非出願対象技術としては、①侵害特定が出来ないか特定が難しい技術、②市場に出荷される製品から技術の中身が確認できないか推測出来ない技術、③公開しなければ競合他社が模倣出来ないか模倣が困難で、製品の市場優位性を維持できる技術、④製造法、及びその装置に関する技術、⑤化学中間材料（中間体）、等が挙げられる。

非出願対象技術として、営業秘密管理対象にして不正競争防止法で保護するには、その技術が、営業秘密の要件、即ち、①秘密管理性（秘密に管理されている）があること、②有用性（事

業活動に有用な技術上又は営業上の情報）があること、③非公知性（公然と知られてない）であること、が満たされて管理されていなければならない。しかも、不正競争防止法で保護されるには、その技術が文字通り不正に流出或いは不正に漏洩した場合に限られるが、不正に流出或いは漏洩したことを立証するのが困難な場合が多い。又、営業秘密管理対象にするということは、「非公知性」を維持することから、同じ技術（発明）が他者から出願される可能性も含んでいる。このリスクを回避する対抗手段として日本には先使用権制度が特許法等には設けてあるが、後に述べるように使い勝手がよい訳ではない。

企業においては、職務発明問題の観点から会社が譲渡を受けるか受けないかを定める必要がある発明（技術）に検証困難な発明（技術）があり、譲渡を受けるとした発明（技術）は、非出願対象技術の一つとして管理される。

図7に、検証困難な発明（技術）の取り扱いの一例が示される。

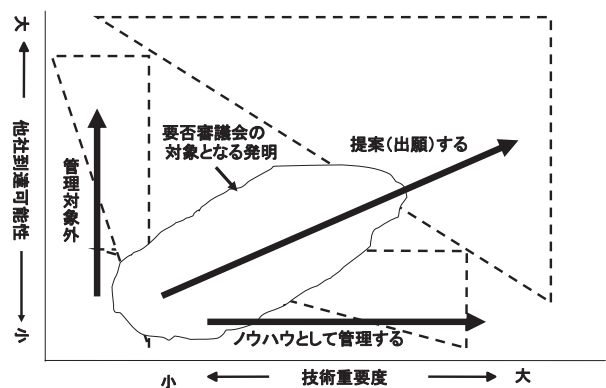


図7 検証困難な発明の取扱

横軸は、技術の重要度であり、図の右に進むほど重要性は高まる。縦軸は、他社（者）が同じ発明（技術）を思い着くまでにどの程度の経過が必要とされるかを示すもので、図の上に進むほどその発明（技術）を着想するのに時間が必要であることを示す。図では、検証困難な発



**本文の複製、転載、改変、再配布を禁止します。**

明（技術）の取り扱いとして、4つの領域に大きく分けてある。図左サイドの領域は、明らかに管理対象外の発明であり、会社として発明者から譲渡を受けない発明である。図下部の領域は、所謂「KH」として管理する発明の領域、上部右サイドの領域は、出願する発明の領域である。これら3領域で囲まれた領域の発明は、これら3領域の何れの発明として取り扱うかを発明取り扱い審議会で審議する対象の発明である。審議会は、洞察力に長けた、技術に明るい技術専門家で構成される。

**2. 3. 7 日本の先使用権制度**

日本における先使用権制度の設置の趣旨は、図8<sup>14)</sup>に示す通り、先願者の出願時以前から事業を準備していた者或いは事業をしていた者との間の公平さを図るものである。

先願主義を採る特許法においては、複数の者が独立に同一内容の発明をした場合、先に出願した者だけが、特許権を取得できる。詰り、最先の発明者が、必ずしも最先の出願者(先願者)になるものではない。この先願者よりも先に独立して同一内容の発明をした者であっても、先願者の特許権に服さなければならぬのが大原則である。

そこで、先願者の特許出願時以前から、独立して同一内容の発明を完成させ、その発明の実施である事業をし、あるいは、その実施事業の準備をしていた者(先使用者)は、法律の定める一定の範囲で、先願者の特許権を無償で実施(先使用者は、通常の実施権を有する)し、事業を継続できる、として、両者間の公平を図ろうとするもの

<sup>14)</sup>「先使用権制度の円滑な活用に向けて」より、一部変更して引用

**図8 先使用権の趣旨**

日本の特許法には、第79条に「先使用権による通常実施権」が規定されてあるが、同様な制度が、実用新案法、意匠法でも認められている。

図9に特許法第79条を分かり易く分節して示す。

先使用権の立証は、特許出願時の先使用を立証するものであるが、その巧拙は、立証の準備如何による。どのような証拠物件を、どの様にして、どう保管するかが決め手になる。

立証において大事なものは、図9に示す①から

①先使用発明の知得経路	特許出願に係る発明の内容を知らないで自らその発明をし、又は特許出願に係る内容を知らないでその発明をした者から知得して、
②特許出願の際に、	
③日本国内において、	
④実施又は準備	その発明の実施である事業をしている者又はその事業の準備をしている者は、
⑤先使用権の範囲	その実施又は準備をしている発明及び事業の目的の範囲において
⑥その特許出願に係る特許権について通常実施権を有する	

**図9 (日本) 特許法79条**

④に至る経緯を立証出来ることである。立証に必要なとする証拠の確定には、物件とその日付の特定とが必要であり、最近のように書類等が電子ファイル化されている場合が多いことから、証拠物件として電子公証した電子ファイルを、電子認証或いはタイムスタンプを活用して日付を特定することが推奨される。図9の①から④に至る経緯を立証するのに必要な証拠物件としては、先使用発明に至る研究開発行為に関する事、先使用発明の完成又は発明者からの知得に関する事、先使用発明の実施である事業の準備に関する事、先使用発明の実施である事業の開始に関する事、を証明する物件であり、それらを証拠として確定しておくことが企業においては技術管理上重要なことである。

収集する証拠物件に必要なことは、各証拠物件が納得性ある流れで証明できるストーリー性を構築できるものになっていることである。各証拠物件の証拠性の確保には、集める証拠は、①誰のもので、②どのような内容であり、③何時から存在し、④その後一切改竄されていない、ことを立証することが必要である。

立証しようとする先使用発明によっては、証拠物件として、電子書面だけでは立証不十分といわれるのを避けるためにビデオやスチール写真を用意することも必要である。

証拠物件を確定した後は、その保管にも注力が必要である。例えば、電子ファイルを電子公

## 本文の複製、転載、改変、再配布を禁止します。

証して証拠物件とするには、長期間において検証可能としておかなければならない。特に、閲覧ソフトは、長期間（継続性）に渡って提供されることが必要である。電子証拠物件そのものの保存には、セキュリティだけでは不十分であり、ファイルサーバーの維持、定期的なバックアップファイルの作成等運用面で解決しておく必要がある。更に、地震、台風、竜巻、火山噴火などの天災や火事などの人災の対策に、オンラインストレージ等の外部遠隔地へのデータ保管が必要である。

証拠が、デジタルデータで、メンテナンスが必要になる場合は、公証役場で、事実実験公正証書を公証人の前で開封してダビングすることになる。その後の扱いは、初度と同じ手続きをすればよいことになる。又、デジタルデータで証拠を保管する場合は、その閲覧性と検索性に優れたソフトを使用することである。そのようなソフトの代表の一つとして、PDFが挙げられる。PDFは、継続性があるだけでなく、例えば、添付ファイルの機能や検索機能があるので便利である。CADデータ、プログラムファイル、映像データ等、関連技術資料をまとめて一つのPDFに添付できる（電子包帯の機能）し、簡単に検索も出来る。

有効な証拠資料になるものとしては、研究ノート、打ち合わせ議事録、技術成果報告、設計図、仕様書、事業計画書、事業開始決定書、見積書、契約書、請求書、納品書、帳簿類、作業日記、カタログ、パンフレット、商品取扱説明書、製品サンプル、写真やビデオ撮影した映像、等々が挙げられる。これらは、公証時点で存在の日付を確保できるが、立証時点が公証時点より遡及する必要が生じることを予測して、作成時に日付を入れておくのが上策である。

先使用権の要件を備えるための証拠を確保するタイミングと他社の特許出願や特許権を知った際の対処の仕方も、技術管理上重要なことで

ある。

証拠は、基本的には、以下の段階ごとに日々作成される資料から確保する。必要な時は、改めて、写真撮影やビデオ撮影をして証拠資料とする。

- ・研究・開発段階
- ・発明の完成段階
- ・事業化に向けた準備が決定された段階
- ・事業の準備段階
- ・事業の開始及びその後の段階
- ・実施形式などの変更の段階

他社の特許出願や特許権を知った際の対処の仕方は、まず、「他社の特許出願や特許権」の内容を検討し、それまでに保管してある証拠で充分かどうかを確認する。確認の結果、不十分な場合は、証拠を再収集する。立証するのに証拠が不十分かどうか判断をし兼ねる際は、迷うことなく証拠の再収集と新たに収集した証拠の証拠能力の確保に努めるべきである。特に、他社の特許権を知った時は、その特許権の出願日と先使用権の要件を備えるための証拠能力を担保した時点がかなり離れている場合が多いので、証拠の中には、その特許権の出願日に日付が間に合っていないこともあり得る。従って、上記各段階での証拠資料は、日付が出来るだけ遡及しているものから選択するのが最善である。

先使用権を主張する者は、他の者の特許出願後には、実施行為の変更、追加が出来ないことも心しておく必要がある。勿論、ここでいう実施行為は、特許法第2条3項に記載された行為である。

又、相手側から特許により権利侵害で権利主張された際、先使用権の存在を示すことで反論すると、先使用とする自身の発明（技術）が相手の権利範囲に属することを自認することになるので、先使用権による反論は、慎重にすべきである。若し、先使用権の立証に不備を来たす

**本文の複製、転載、改変、再配布を禁止します。**

と侵害自認だけが残るので、先使用権による反論は、最後の最後にすべきである。

**2. 3. 8 日本以外の国での先使用権制度**

米国における先使用権制度は、米国特許法の第273条に記載されているが、もともとの米国特許法にはこの条文はなく、ビジネスモデル特許が囃された頃に新たに追加されたものである。ビジネスモデル特許の場合、特許発明以前から同一の発明があったであろうことの蓋然性が高いにも拘らず証拠が発見されずに特許が成立することが多かったため、商業的に先実施していた者の救済の意味で例外的に設けた条項である。特許発明の有効な出願日より1年を超える以前に善意で発明を完成し、特許発明の有効な出願日より前に商業的に実施していた者は、拳証責任を負うが特許侵害からは救済される。ただ、救済される実施行為は、ビジネスの実施方法と運営方法の使用に限られる。又、特許侵害と主張された特許発明の主題の使用を放棄と見做される中断を行うと、放棄日より後に

提訴された事件において、放棄日より後の行為について、本条の抗弁を立証するにあたり、放棄日より前に行った活動を根拠とすることは出来ない。

中国では、専利法の第63条（特許権の侵害と見做さない行為等）2項に記載がある。中国の先使用権制度では、実施行為は、製造の発明と方法の発明の使用に限られるが、企業にとっての一番の問題は、従来の範囲内での製造、使用でしか継続出来ないことである。企業である以上生産の拡大は事業発展と共に至極当然であるにも拘らず、生産拡大が先使用権で保護されないとすると実務的には先使用権制度がないのと同じである。

韓国では、特許法の第103条（先使用による通常実施権）に記載があり、冒認発明も先出願として認めるようで、先使用権制度のある主要国の中で制約が一番少ない国である。その他の国の先使用権制度の概略が図10にまとめて記載してある。

先使用権の立証の仕方となると、それぞれの

国	該当条文	先発明の対象	基準日	善意の要件	継続の要件	効果	移転
タイ	36条(2)	特許製品/ 特許方法	出願日 (優先日ではない)	要	不要	製造/方法の使用が可能。	
フィリピン	73条 (先使用者)	当該発明	出願日 (優先日)	要	要	発明の使用を継続する権利を有する。	企業/営業の一部とともに移転/譲渡可能。
インド	24B条(排他権の付与)(2)	発明に係る物品/物資	出願時	不要	不要	販売/頒布は排他権の侵害とはみなさない。	
インドネシア	13条	同一の発明	出願時	不要	要	発明を実施する権利を有する。	
英国	64条	発明	優先日	要	要	侵害に該当する行為を引き続き実行し又は自らこれを実行する権利を持つ。	
独国	12条	その発明	出願時	要	不要	特許の効力はその発明を実施していた者又は実施のために準備をしていた者に対しては及ばない。	事業とともにのみ相続/譲渡可能。
仏国	L613-7条	特許権の主題である発明	特許出願日又は優先日	要	不要	個人的に実施する権利を有する。	事業又はその事業の一部とともにのみ移転可能。
中国	63条(権利侵害とみなされる行為)1項2号	同一製品/方法	出願日	不要	要	権利侵害とみなさない。	
韓国	103条(先使用による通常実施権)	実施/準備をしている発明	出願時	要	要		

図10 日米以外での先使用権の概要

## 本文の複製、転載、改変、再配布を禁止します。

国の公証制度も区々で不明な点が多く、証拠の保全もその仕方も、現地の弁護士に問い合わせても弁護士によって色々な回答をして来るので、どの回答がもっともなのか判断し兼ねる場合が少なくない。

### 3. 中国における営業秘密

#### 3.1 中国の営業秘密の要件と労働者対策

中国における営業秘密の要件は、日本におけるのと然程変わらない。

第一の非公知性の要件には、①権利者が主観的に秘密保持の意志を有し、秘密保持の対象の情報を、通常の公開ルートでは知ることができない状態で機密保持する然るべき秘密保持措置をとっていると主観性を具備すること、②秘密保持の対象の情報が、客観的に公衆に知られていない、またはパブリックドメインに入っていないことの客観性を具備することが、必要である。

第二の要件は、権利者に経済的な利益を齎すことができ、実用性があることであり、権利者に現実的または潜在的な経済的利益または競争の優位性を齎す経済的価値を有することである。この経済的価値は、権利者が認識するだけでなく、客観的にも実用的価値を備えていることが必要である。

第三の要件は、損失金額要件である。営業秘密の侵害行為を行い、権利者に多大な損害を齎して初めて犯罪を構成するので、損害損失がそれ程深刻でない程度の場合は当該犯罪を構成しない。

労働法における企業の営業秘密保護には、秘密保持制度の確立と労働者との秘密保持契約がある。

秘密保持制度の確立には、(1)物に対して、①工場・生産区域の秘密保持、②生産の設備・過程の秘密保持、③原材料・金型に対する秘密

保持、④文書・コンピュータに対する秘密保持、⑤廃棄物に対する秘密保持などがあり、(2)人に対して、①部外者の秘密保持管理、②社員の秘密保持管理(秘密保持契約、競業禁止契約以外の)、③退職従業員の資料返却秘密保持管理などがある。

労働法22条には、「労働契約当事者は、労働契約中に企業の営業秘密保持に関連する事項を約定することができる」と規定されているが、企業は、労働契約以外に別途秘密保持契約を締結して企業と労働者との権利義務関係を約定することが必要である

企業は、労働者が企業を辞める際には、誓約書を交わして競合相手に再雇用されないように若しくは協業を起業しないように協業禁止を約定するのが賢明である。「科学技術者流動における技術秘密管理の強化に関する若干意見」第7条では、競業禁止条項の年数制限(3年以内)と競業禁止期間の補償費用について規定している。同条では、違反若しくは補償費用の支払いを怠ると競業禁止条項は自動的に直ちに終了することになっているので、企業は、その履行に注意が必要である。

「労働契約法」(2006年3月20日公布)第16条では、競業禁止期間は2年以内、経済補償は年収以上と規定され、労働者が違反すると使用者が支払う経済補償の3倍以内の違約金を使用者に支払わなければならないことになっている。

#### 3.2 日本の不正競争防止法での中国における営業秘密侵害対策

営業秘密侵害の類型は、不正競争防止法第2条1項(営業秘密を侵害する行為)、同条同項4-6号「不正取得による侵害型」、及び同条同項7-9号「不正取得後の背信侵害型」に示され、差止請求、損害賠償請求ができることになっている。又、国外犯罪処罰規定(平成17年改正)には、「詐欺等の行為若しくは管理侵害行為が

## 本文の複製、転載、改変、再配布を禁止します。

あった時または保有者から示された時に、日本国内で管理されていた営業秘密について、日本国外でこれらの罪を犯した者」にも適用できるとされる。そしてその罰則は、5年以下の懲役若しくは500万円以下の罰金が科され、行為者の法人に対しても、1億5千万円の罰金を科すことが出来る(両罰規定)。しかし、日中間では、犯罪人引渡し条約が未締結であるので、被疑者が中国国内にいる場合は、適用が難しくなる。

更には、準拠法の問題がある。

日本の裁判所での場合は、日本の「法例」に従い、契約の成立と効力は、当事者の意思に従い、当事者の明示の意思が明らかでない場合は、黙示の意志に従う。それでも明らかでない場合は、行為地法による。債権の成立と効力は、その原因たる事実の発生地法による。

中国の人民法院での場合は、中国の「民法通則」に従って決定される。契約者は、紛争処理に適用する法律を選択できる(民法通則145条1項)。選択されてないときは、契約と最も密接に関係する国の法律が適用される。当事者双方が同じ国籍または住所を有する場合は、当事者の本国法または住所地法が適用される。前記の「不法行為地の法律」は、「不法行為が行われた地の法律」と「不法行為の結果が発生した地の法律」の両者を含む。

## 4. あとがき

技術の流出防止は、企業の事業戦略上大事なことである。どの技術をどの様に流出防止するのか、その技術は新規なのかそうでないのか、流出防止策の実践を関係者にどう徹底させ、その徹底をどう管理するのか、その巧拙如何では企業の存亡を左右し兼ねない。

しかし、いくら厳重に管理しても流出を防止する技術に人が関与している限り、流出を完全に防止することは不可能である。一旦、人の記憶に留まった技術は、人と共に流動する。退職

者に誓約書等で誓約させて安心している企業が多いが、技術に關与していた人の中から退職者が出た時点で、その技術は流出防止の管理下から外れたことに等しく、キー技術であれば、いつでも流出することを前提に事業戦略を再構築しておく必要がある。況してや2次、3次流出となると流出を立証することすら困難を極める。仮に流出が立証できたとしても、一旦渡った技術は、返還請求して取り戻したとしても、依然として流出先の人の記憶に残り実質的には完全に取り戻すことが出来ない。流出先企業の流出技術に關与した人を自社の管理下におくことで完全返還を図ることも理論的には考えられるが、実効性に乏しい。精々、損害賠償請求や使用差止請求をするしか効果的な法的手段を取る道はない。況してや流出技術に改良や変更を加えて使用されると、立証が一層難しくなる。

技術を営業秘密として守るとなると、管理負荷が大きくなり、管理を厳重にすればする程管理システムは複雑になり大きくもなる。また、利便性のためにネットワーク化を図るとサイバーアタッカーの脅威に晒される。

特許出願で技術保護を企てると属地主義と世界同時公開性が問題になるが、基本的には出願国の選定のリスクを負うことで済む。出願国の問題は、当初から知れていることなので、事業上での特許取得コストと世界同時公開性ととのバランスで出願国を決めれば済むことである。特許取得による技術保護の場合は、出願当初より問題が顕在化しているのに対して、営業秘密として保護する場合は、問題が潜在しており且つ何処の国・地域でいつ起こるかが不確定であるところに大きな問題がある。加えて、特許取得による技術保護の場合は、記載要件を満たした上で出願明細書やクレーム(特許請求の範囲)の書き方を工夫したり多重出願したりすることで、出願明細書やクレームが公開されても保護

## 本文の複製、転載、改変、再配布を禁止します。

する技術を競合相手が習得するのを防止することが出来る。将に、出願戦略の妙である。昨今のように、誰でも（素人でも？）一読すれば解るように出願明細書やクレームを書きましようとか、機械翻訳を前提にした日本文の簡単明瞭化（又は簡素化）の動きは、企業の出願戦略の高度化の知力を阻害して、出願戦略の画一性と一様化を招き日本企業の国際競争力を低下させる。出願の明細書やクレームは、その技術分野の当業者が理解できるように記載すれば法的記載要件を満たすものであって、その技術分野の当業者の全ての者が理解できるように記載する必要はない。今や企業にとって、特許法における技術公開は、技術振興のための公開ではなく、保護すべき技術が競合に容易く読み取られないように出願の明細書やクレームの記載を創意工夫して、目的の排他的独占権を得るための一手段に過ぎなくなりつつある。

しかも真に大事なものは、出願の公開による技術の流出自体ではなく、技術のリードタイムをいつまでとれば競争優位が維持できるか、その間に次世代技術が開発できるか、である。技術のリードタイムの開始時点とリード期間の設定は、競争優位戦略の重要なファクターである。出願戦略の妙は、自社の競争優位を確保・維持するために、特許権で保護すべき技術のリードタイムの開始時点とリード期間を如何に設定するか、出願の明細書やクレームの記載の創意工夫と出願のタイミングを図ることにある。

次世代技術が開発され、その技術を使用する製品の量産見込みが就いたら、現世代の技術は戦略的に供与してグループ作りをすることで、技術囲い込みをするのも一つの事業戦略である。日本が技術流出防止一点張りである間に韓国は、技術流出防止にはそれ程重きを置かず、マーケットの獲得と支配とに視点を置いて、インド、ロシア、中国、ブラジルなどの大型市場を席卷しようとしている。

技術の流出防止に明け暮れて、マーケットを奪われては元も子もない。今や日本は、政治の内輪もめをしているのではなく、国際競争に強い日本の産業を育成するために政産学官のそれぞれが智慧を結集して何をすべきか政策を立て実践しなければならない時期にきている。それには、国民やマスコミがもっと真剣に日本の将来を考えなければならない。

### 注 記

- 1) 経済産業省、「技術流出防止指針～意図せざる技術流出の防止のために～」(平成15年3月14日), <http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/030314guideline2.pdf> (参照日: 2011.2.14)
- 2) 経済産業省、「技術流出防止指針～意図せざる技術流出の防止のために～関連参考資料」(平成15年3月14日), <http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/030314jirei.pdf> (参照日: 2011.2.14)
- 3) 経済産業省、「営業秘密管理指針」(平成22年4月9日改訂), <http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/hontai0409.pdf> (参照日: 2011.2.14)
- 4) 首相官邸セキュリティ対策推進会議決定、「情報セキュリティポリシーに関するガイドライン」(平成12年7月18日), <http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html> (参照日: 2011.2.14)
- 5) 経済産業省、「情報セキュリティ管理基準」(平成20年改正版), [http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS\\_Management\\_Standard.pdf](http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard.pdf) (参照日: 2011.2.14)
- 6) 通商産業省告示536号(最終改正)、「情報システム安全対策基準」(平成9年9月24日), <http://www.meti.go.jp/policy/netsecurity/downloadfiles/esecu03j.pdf> (参照日: 2011.2.14)
- 7) 通商産業省告示952号(最終改定)、「コンピュータウイルス対策基準」(平成12年12月28日), <http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm> (参照日: 2011.2.14)
- 8) 通商産業省告示950号(最終改定)、「コンピュー

## 本文の複製、転載、改変、再配布を禁止します。

- タ不正アクセス対策基準」(平成12年12月28日),  
<http://www.meti.go.jp/policy/netsecurity/UAaccessCMG.htm> (参照日:2011.2.14)
- 9) 国家公安委員会告示第19号 (一部改正),「情報システム安全対策指針」(平成11年11月22日),  
[http://www.npa.go.jp/cyber/policy/antai\\_sisin/kokuji.htm](http://www.npa.go.jp/cyber/policy/antai_sisin/kokuji.htm) (参照日:2011.2.14)
- 10) 典型的なマネジメントサイクルの1つで,計画(plan),実行(do),評価(check),改善(act)のプロセスを順に繰り返し実施すること。
- 11) 特許庁総務部企画調査課,「先使用権制度ガイドライン(事例集)「先使用権制度の円滑な活用に向けて一戦略的なノウハウ管理のために一」について」(平成18年6月16日),  
[http://www.jpo.go.jp/shiryous/s\\_sonota/senshiyouken.htm](http://www.jpo.go.jp/shiryous/s_sonota/senshiyouken.htm) (参照日:2011.2.14)
- (2) 経済産業省,「2010年版ものづくり白書」(2010) 経済産業調査会
- (3) 経済産業政策局知的財産政策室,「産業構造審議会 知的財産政策部会 経営・市場環境小委員会(知的財産の取得・管理指針,営業秘密管理指針,技術流出防止指針,特許・技術情報の情報開示のパイロットモデル,知的財産権の信託に関する緊急提言)」(平成15年3月)  
<http://www.meti.go.jp/report/data/g30314aj.html> (参照日:2011.2.14)
- (4) 経済産業省,「我が国における技術流出及び管理の実態について」(平成19年6月)  
<http://www.meti.go.jp/committee/materials/downloadfiles/g70625a05j.pdf> (参照日:2011.2.4)
- (5) ジェトロ北京センター 知的財産権部,「中国における営業秘密 保持と技術流出防止」(2006年3月31日),  
[http://www.jetro-pkip.org/upload\\_file/2007033033869641.pdf](http://www.jetro-pkip.org/upload_file/2007033033869641.pdf) (参照日:2011.2.14)

### 参考文献

- (1) 射手矢好雄,遠藤誠,「中国における技術流出及び営業秘密侵害とその対策」(2005) 日本機械輸出組合

(原稿受領日 2011年1月19日)

