HOKKAIDO UNIVERSITY

Title	営業秘密における秘密管理性要件
Author(s)	津幡, 笑
Citation	知的財産法政策学研究, 14, 191-213
Issue Date	2007-03
Doc URL	https://hdl.handle.net/2115/43515
Type	departmental bulletin paper
File Information	14_191-213.pdf

Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP

営業秘密における秘密管理性要件

津　幡　　笑

一　はじめに

不正競争防止法により営業秘密として保護されるためには、(1) 秘密管理性（2）有用性（3）非公知性の 3 つの要件を満たさなくてはならない。

とりわけ注目すべき要件は「秘密管理性」であり、この点に関する企業の努力は大きな意味を持つ。経済産業省報告書「電気電子産業における営業秘密保護について」によると、営業秘密の 3 要件（秘密管理性、有用性、非公知性）に関して、全回答企業の79%が「知っている」と答えたが、重要情報について「実務で適切な管理が実行されているか」との問いには、「管理が行われているものとそうでないものがある」との回答は全体の65%に及び、19%の企業は「要件を満たす管理がほとんど行われていない」と答えた。一方、「ほとんどすべての重要情報が管理されている」との回答は14%に留まった[1]。

それでは具体的に、企業に望まれる営業秘密の管理水準はいかなるものであるべきか。

一つの基準となるのが、経済産業省が2005年に公表した『企業における適切な営業秘密管理指針-平成17年不正競争防止法改正・営業秘密管理指針改訂-』[2]（以下『営業秘密管理指針改訂版』という）である。これは企業が営業秘密を管理する際の参考となるガイドラインで、最初の『営業秘

[1]「経産省、『電気電子産業における営業秘密保護に関する調査』を公表（上）」知財Awareness2006年7月28日付記事<http://chizai.nikkeibp.co.jp/chizai/gov/20060728.html>(2006年11月28日 最終確認)

[2] 経済産業省知的財産政策室編『企業における適切な営業秘密管理指針-平成17年不正競争防止法改正・営業秘密管理指針改訂-』（経済産業調査会・2006年）

密管理指針』は2003年１月30日に公表された。『営業秘密管理指針改訂版』は、改正された不正競争防止法（2005年11月１日施行）に沿い、産業構造審議会知的財産政策部会の委員会が検討を加え、内容を一新したものである[3]。

その内容は、最低限必要な管理の水準として、最近の裁判例の動向を概観した上で、情報自体についての物理的、技術的な管理及び人の管理、さらにはそれらを実効的に行うための組織的な管理について、望ましい管理水準も含めて示すものであるとされる[4]。

しかしながら、後述するように、その内容は、ガイドラインの性質上、高度な水準を企業規模等に関わりなく一律に課すものとなっており、またミニマムな水準としての裁判例の分析も、どういった事実が判決の結論に影響を与えたかという視点がなく、秘密管理性肯定例・否定例から平面的に事実を抽出したにとどまるものである。

そこで、本稿は、『営業秘密管理指針改訂版』の以上のような問題点を踏まえ、裁判例の分析を改めて行うことにより、裁判例における秘密管理性要件の基準を明らかにすることを目的とするものである。

二　学説

学説によると、秘密管理性要件を満たした状態とは、情報にアクセスする者から客観的に秘密として管理されていると認められる状態をいうとされ[5]、一般的な管理方法としては①客観的な認識可能性②アクセス制限の２つが挙げられることが多い[6]。しかし、「客観的」という文言は多義的

[3] 従来の企業における営業秘密の管理方法に関する指針に加え、企業が退職者との間で結ぶ秘密保持契約のあり方、法人に対する処罰に関して前提となるべき企業の選任監督義務などに関する方針が盛り込まれた。

[4] 経済産業省知的財産政策室・前掲注2、23頁。

[5] 金井重彦＝山口三恵子＝小倉秀夫編『不正競争防止法コンメンタール』[山口三恵子]（レクシスネクシスジャパン・2004年）166頁。

[6] 竹田稔『知的財産侵害要論[不正競業編]』(改訂版・発明協会・2006年)148頁、松村信夫『不正競業訴訟の法理と実務』（第４版・民事法研究会・2004年）381頁、三

に評価されうるものであり、また、誰にとって客観的といえるかについてはあまり論じられてこなかった[7]。

そのような状況下でも、秘密管理性の趣旨から具体的な判断基準を導く見解が従来から唱えられてきた。すなわち、秘密管理性要件が設けられた趣旨を、情報の利用者に対して保護されている情報の識別を容易にするところに求めた上で、同要件の充足の有無を判断するためには、不正手段を用いて秘密を取得しようとしている者（２条１項４号）、秘密の開示を受けた者（２条１項７号）、あるいは秘密を保持する義務を負っている者（２条１項８号）が秘密であると認識できる程度に管理されているか否かを基準とすべきとする見解である[8]。この見解によると、秘密管理は相対的な概念であり、管理方法について統一的な基準があるわけではなく、個々のケース毎に判断していくことになる。窓から入ってくる侵入者に対しては、情報を記載した書類を机の引き出しに入れておくだけで十分というべき

山峻司＝松村信夫『実務解説知的財産権訴訟』（第２版・法律文化社・2005年）379頁、末吉亙編『実務知的財産法講義』［末吉亙］（民事法研究会・2005年）479頁、青山紘一『不正競争防止法（事例・判例)』（経済産業調査会・2002年）97頁、小野昌延＝山上和則編『不正競争の法律相談』[小原正敏]（青林書院・1997年）257頁、角田政芳＝辰巳直彦『知的財産法』（第3版・有斐閣・2006年）249頁、土肥一史『知的財産法入門』（第9版・中央経済社・2006年）18頁、小野昌延『新・注解不正競争防止法』[小野昌延]（青林書院・2000年）513頁、千野直邦『営業秘密の法的保護』（中央経済社・2002年）154頁。

[7] 客観的に認識可能であるかどうかは、不正行為者との関係で相対的に決まるとするものとして渋谷達紀「営業秘密の保護・不正競争防止法の解釈を中心として」法曹時報45巻2号6頁（1993年)。秘密管理性の内容として主観的要件と客観的要件を要求するものとして、山本庸幸『要説不正競争防止法』（第4版・発明協会・2006年）138頁。

[8] 田村善之『不正競争法概説』(第2版・有斐閣・2003年)330頁、渋谷達紀『知的財産法講義（3)』(有斐閣・2005年)107頁、相沢英孝＝西村ときわ法律事務所編『知的財産法概説』[川合弘造]（第2版・弘文堂・2006年）330頁、茶園成樹「営業秘密の民事上の保護」日本工業所有権法学会年報28号40-41頁(2004年)、苗村博子「技術ノウハウ（営業秘密）の秘密管理性を認めなかった高裁決定」知財管理52巻9号1354頁(2002年)、苗村博子＝重冨貴光「営業秘密について」パテント55巻1号14頁(2002年)。

であるが、通常は書類を自由に閲覧しうる社内の従業員に対しては、書類にマル秘マークを付しておくとか、ロッカー内に施錠して保管することが必要となる[9]。

他方、立法担当者は秘密管理性要件をどのように考えていたのであろうか。通商産業省の当初の解釈によると、「①当該情報にアクセスした者に当該情報が営業秘密であることを認識できるようにしていることや、②当該情報にアクセスできる者が限定されていること」が必要であるとされ[10]、上述の秘密管理性を相対的にとらえる説と親和的であったかのようである。しかしながら、現在の『営業秘密管理指針改訂版』によると、前記の2要件に加えて、「秘密管理性が認められるためには、事業者が主観的に秘密として管理しているだけでは不十分であり、客観的にみて秘密として管理されていると認識できる状態にあることが必要である」[11]とされ、客観的な認識可能性を要求しているところに変化が見られる。ただし、前記学説の紹介でも述べたように、「客観的」という言葉をもってして誰にとって客観的なのかは明確ではなく、上述の相対的に秘密管理性をとらえる見解を否定したものとまではいえないであろう。

三　裁判例

（一）営業秘密管理指針における裁判例の分析

それでは、裁判例において秘密管理性はどのようにとらえられているのであろうか。

『営業秘密管理指針改訂版』は、裁判例の分析から「営業秘密が不正競争防止法上の保護を受けるために必要な秘密管理性に関し、事業者が主観的に営業秘密と考えているだけでは足りず、①情報の秘密保持のために必要な管理をしていること（アクセス制限）②それが（アクセスした者に）客観的に秘密であると認知されること（客観的認識可能性）を必要としている」と述べる[12]。

そして、①に関しては、施錠の有無、パスワードの設定などがあり、②については、他の一般情報との区別、秘密である旨の表示などが具体的な判断要素となっているが、それを実質的な観点から整理すれば、全般的には以下の三点に着目して関して判断が行われているとされる。

A．アクセスできる人が限定され、権限のない者によるアクセスを防ぐような手段が取られている

B．アクセスした人が、管理の対象となっている情報をそれと認識し、またアクセス権限のある人がそれを秘密として管理することに関する意識を持ち、責務を果たすような状況になっている

C．それらが機能するように組織として何らかの仕組みを持っている（組織的管理）[13]

以上の分析は妥当であろうか。

（二）裁判例における秘密管理性要件の定義

裁判例においては、まず、一般論として「秘密として管理されている」といえるためには、(1) 当該情報にアクセスした者に当該情報が営業秘密であることを認識できるようにしていること、(2) 当該情報にアクセスできる者が制限されていること、が必要であるとするものが多い（東京地判平12・9・28判時1764号104頁［プロスタカス］、東京地判平12・12・7判時1771号111頁［車両変動状況表］、東京地判平15・11・13平成12(ワ)22457[ハンドハンズ終局判決]ほか）。この点については、学説および営業秘密管理指針と共通するところである。

（三）裁判例の秘密管理性判断における具体的要素

それでは、具体的にはどのような事情があれば秘密管理性が肯定されるのであろうか。以下に述べるように、裁判例は（1）秘密管理が厳格に行

[9] 田村・前掲注8、329頁、鎌田薫「『財産的情報』の保護と差止請求権(4)」Law&Technology10号24頁(1990年)。

[10] 通商産業省知的財産政策室監修『営業秘密・逐条解説不正競争防止法』(有斐閣・1990年）55頁。なお同書158頁以下の産業構造審議会報告書『財産的情報に関する不正競争行為についての救済制度のあり方について』も参照。

[11] 経済産業省知的財産政策室・前掲注2、7-8頁。

[12] 経済産業省知的財産政策室・前掲注2、24頁。

[13] 経済産業省知的財産政策室・前掲注2、24頁。

われていて秘密管理性が明らかに肯定されるような事案、(2) 秘密管理が緩く秘密管理性が否定される事案、(3) 前記 (1)、(2) の中間的な事案で、肯定例、否定例がわかれている場合の３つに大きく分けられよう。

(1) 秘密管理性が肯定される例

秘密管理性が肯定されるような事案では、秘密情報が特定され、情報が紙媒体の場合には、施錠、持ち出し禁止などの管理がされていること、情報がデータの場合には、パスワードでアクセス制限がされていることが挙げられているといえよう。

例えば、紙媒体の輸入先目録、顧客目録について、「秘」の印を押印した上で秘密書類保管庫に施錠保管し、鍵は代表取締役が管理しており、謄写も許されていなかった事例では、秘密管理性が肯定されている（東京地判平17・6・27平成16(ワ)24950[中国野菜輸入先・顧客名簿])。顧客情報のデータベースへのアクセスを毎月変更される個別のパスワードにより管理し、ディスプレイ表示も各部門が必要とする最小限度の顧客情報を表示するようなシステムを採用しており、プリントアウトにも関係役員の押印のある依頼書を必要とし、その操作手続を知る者も３名に限定し、印字された名簿を外部に持ち出す場合には社長決裁を必要としているという事案で秘密管理性が肯定されている（東京地判平11・7・23判時1694号138頁［美術工芸品］)[14]。設計業務に必要な範囲内でのみメインコンピュータのサーバーに保存されている電子データにアクセスし、必要な電子データのみを各コンピュータ端末機に取り出して設計業務を行っていたこと、メインコンピュータのサーバー及び各コンピュータ端末機を外部に接続せず、インターネット、電子メールの交換など外部との接続は、別の外部接続用コンピュータ1台のみを用いて行っていたこと、バックアップ作業は、設計部門と営業部門の総括責任者だけに許可されており、作業に当たっては、ＩＤとパスワードをメインコンピュータに入力することが必要であったこと、バックアップを取ったＤＡＴテープは、設計部門の総括責任者の机上にあるキャビネットの中に施錠して保管していたことを斟酌して秘密管理性を認めたものがある（大阪地判平15・2・27平成13年(ワ)10308[ジーティー・ジャパン])。データへのアクセスにはＩＤとパスワードが必要であり、バックアップは責任者が保管しており、また外部に図面が示される場合は決済を経て「Confidential」の印を押し、秘密保持契約を締結していた事例では、秘密管理性が肯定されている（福岡地判平14・12・24判タ1156号225頁[CAD データ])。また、20万人余りの顧客情報に関して、その元となる個々の情報自体は社内のコンピュータにアクセスして１件ごとに出力することは理論的に可能であるが、5段階の手順と異なる処理名を入力する必要があり、作業にはかなりの時間を要するから、実際にはパスワードが幾重にも設定されていることと同じ効果がある、として秘密管理性を肯定する判決がある（他の厳重な秘密管理体制の状況をも斟酌して、東京地判平12・10・31判時1768号107頁［放射線測定機械器具］)。

他に従業員に秘密保持義務を課すことによって秘密管理性を認めた例として、新規採用社員に対して、原告が保管する営業資料について、営業活動以外への使用の禁止を指導していた例（東京地判平12・11・13判時1736号118頁［来山者名簿]）[15]、就業規則で、従業員に対し、会社の業務上の秘密を他に漏らさないことを義務づけ、新入社員の入社時にもその旨指導するなどしていた例（東京地判平16・5・14平成15(ワ)5711[作務衣]）がある。

(2) 秘密管理性が否定される例

逆に、情報媒体の施錠管理、持ち出し制限等がなかったり、パスワードによるアクセス制限がない等、誰から見ても秘密でないのが明らかであるような場合には、秘密管理性が否定されている。

例えば、コンピュータを操作する者が限定されておらず、パスワードでアクセス制限が掛けられているわけでもない情報や、机上に置かれたり、鍵を掛けていないキャビネットに保管されており、社内の誰もが自由に使用できるファイルや袋に入れられている情報であって秘密の表示のないものは、秘密管理性を否定されている（東京地判平11・5・31判不競1250ノ186ノ12頁［化学工業薬品］)。顧客名簿に秘密とする表示がなく、そのプリントアウトが本立てに置かれており社員が自由に見ることができたという場合も同様である（東京地判平10・11・30判不競1250ノ186ノ6頁［ス

[14] この事案においては、次長という幹部職にある被告の指示で数回、所定の手続が履践されなかったという事情は秘密管理を否定する方向に斟酌されていない。

[15] 工藤莞司「来山者名簿・判批」時の法令1664号61頁(2002年)。

コアーカットナイフホールダー］）。同種の書類中の一部のみに「マル秘」の押印があるにとどまるうえ、同内容の情報がパソコンに保存されており パスワードが設定されていない場合も、他の社内向け文書と大差ない状態で管理されており秘密管理の要件を満たさないとされた（東京地判平12・12・7 判時1771号111頁［車両変動状況表］）（他の否定例に、大阪地判平11・9・14判不競1250ノ186ノ22頁［顧問先名簿］、東京地判平12・9・28判時1764号104頁［プロスタカス］、大阪地判平14・9・26平成13年(ワ)13897[実績管理台帳]、東京地判平17・2・25判時1897号98頁[薬品リスト]、東京高判平17・2・24平成16年(ネ)5334[ペットサロン顧客名簿]、東京地判平18・7・25平成16年(ワ)25672[在宅介護サービス]）。

なお、秘密管理は必ずしも物理的なものであることを要しない。文書化されていない情報に関しては、従業員に対して秘密保持義務を課すだけでも、義務を負っている情報がどれであるのかということが明確であるかぎり、秘密管理性を満足すると解される。もっとも、従業員に一般的な守秘義務があるからといって、何が秘密を守るべき情報なのかということがわからない場合には、結局、秘密管理性が否定される（前掲東京地判［車両変動状況表］）。たとえば、文書化されている情報については、従業員に守秘義務があるというだけでは足りず、当該文書が秘密として管理されている必要がある（前掲大阪地判［顧問先名簿］、大阪地判平10・12・22知裁集30巻４号1000頁［フッ素樹脂シートの溶接技術］）。

(3) 問題となる裁判例

前記（1）、（2）の裁判例をみるに、『営業秘密管理指針改訂版』の分析は一見妥当であるかのようである。指針は、裁判例が、Ａ.アクセスできる人が限定され、権限のない者によるアクセスを防ぐような手段が取られている、Ｂ.アクセスした人が、管理の対象となっている情報をそれと認識し、またアクセス権限のある人がそれを秘密として管理することに関する意識を持ち、責務を果たすような状況になっている、Ｃ.それらが機能するように組織として何らかの仕組みを持っている（組織的管理）ことに着目して判断しているとするが、Ａ.Ｂ.については概ね妥当しよう。また、Ｃ.も（1）の肯定例で情報へのアクセス制限がシステム上行われていた例からみて、判断要素としてＡ.Ｂ.に並ぶものとして挙げることには疑問ではあるが、間違いとは言えないであろう。

しかし、問題となるのは、施錠がない等、管理に一部欠けているところがあるため、誰の目から見ても秘密であることが明らかであるとはいえないが、情報の利用者にとっては秘密であると認識しうるような場合である。このような場合には、裁判例は、秘密管理性を肯定するものと否定するものに分かれている。

(a)情報の管理を一部欠いていたにもかかわらず秘密管理性が肯定された例

例えば、男性用かつらの販売・理容業の支店長が独立に際して顧客名簿を持ち出した事案について、マル秘の印をつけて顧客からは見えないカウンター裏側に収納していた事実をもって、施錠等がなかったが秘密管理性を認めた判決（大阪地判平８・４・16知裁集28巻２号300頁［男性用かつら］）、元専務取締役、営業課長、製造課長らが競業会社を設立し原告の技術ノウハウと同様の製造工程を用いていた例につき、本件技術を用いた作業を納品先社員や工場見学者に見せていた事情があったとしても[16]、役員、従業員から誓約書を徴して営業秘密の保持義務を課し、在庫管理を製造課長が行い、製造課の部室のロッカーにノズル等の治工具やディスパージョンを保管し、技術を管理しているとして秘密管理性を認めた判決(大阪地判平10・12・22知裁集30巻４号1000頁［フッ素樹脂シートの溶接技術］）や、学習塾の就業規則で塾生の名簿等の漏洩が禁止されており、生徒の住所、電話番号その他の情報が記載された個人別成績記録カードのアクセスが制限されていたという事例で、講師の退職時に生徒の住所、連絡先の欄がある生徒一覧表を記した教務手帳の返還を求めていなかったとしても、業務上の必要を越えてこれらの情報を使用することが認められていたことにはならないとして個人別成績管理表につき秘密管理性を否定しなかった決定（大阪地決平７・６・27判不競1250ノ231頁［開成教育セミナー］）がある。さらに、人材派遣業を営む会社の従業員が派遣労働者の雇用契約に関する情報および派遣先の事業所に関する情報を持ち出した事例につき、秘密表示がなく、情報の一時持ち出しが認められていたにもかかわらず、

[16] ただし、作業工程を見せていたとしても、ノズルはさほど大きいものではなく部外者にとっては具体的にどのような加工をしているかを知ることは困難であるとして、営業秘密であることを認めている。

当該情報が記載されたスタッフカードの保管形態、スタッフカードをコピーし保持することは予定されていなかったこと、研修、秘密保持契約で秘密の保持に留意していたことから秘密管理性を認めた判決（東京地判平14・12・26平成12(ワ)21051[ハンドハンズ(中間判決)]、終局判決は東京地判平15・11・13平成14(ワ)21051)、コンピュータに保存されていた設計図の電子データの元エンジニアによる持ち出しが問題となった事案で、パスワード等によるアクセス制限、秘密であることの表示等がなかったにもかかわらず、全従業員数が10名であり電子データの取扱いの態様は従業員の全員に認識されていたものと推認し、性質上情報への日常的なアクセスを制限できないとして秘密管理性を肯定した判決（大阪地判平15・2・27平成13(ワ)10308等[セラミックコンデンサー][17]）がある。

ところで、前述の『営業秘密管理指針改訂版』は、情報の物理的・技術的管理のミニマムな基準として「秘密として管理すべき情報のうち、紙やフロッピーディスク等の記録媒体（有体物）により管理されているものに関しては、秘密として管理する情報とその他の情報を区分した上で媒体に秘密である旨を表示し〔情報の区分と表示〕、その媒体にアクセスできる者を限定〔アクセス制限〕した上で、媒体を施錠可能な場所で管理し、廃棄の際には復元不可能な形にする〔媒体の保管と廃棄〕こと。さらに、その保管場所がある施設について、施錠や入退室の制限を行う〔施設等の管理〕等により管理される」ことを挙げる[18]。

これを前記の裁判例と照らし合わせてみるに、施錠管理、アクセス制限がなかった[男性用かつら]、秘密として管理する情報の区分と表示がなく、施錠・入退室制限がなかった[フッ素樹脂シートの溶接技術]、媒体の保管と廃棄につき管理がなされていなかった[開成教育セミナー]、秘密情報の区分と表示がなく、施錠・入退室制限もなかった[セラミックコンデンサー]は、いずれも営業秘密管理指針に挙げられたような秘密管理水準にはなかったにもかかわらず、秘密管理性が認められた例である。

それでは、これらの事件で秘密管理性が認められた背景にはどのような事情があるのであろうか。[男性用かつら] [フッ素樹脂シートの溶接技術]

[17] 山本英雄「セラミックコンデンサー・判批」知財管理54巻1号69頁(2004年)。

[18] 経済産業省知的財産政策室・前掲注2、27頁。

[開成教育セミナー]事件は情報を持ち出した者自身が情報の管理者であった例であり、[フッ素樹脂シートの溶接技術] [開成教育セミナー]事件は誓約書や就業規則で秘密保持義務が課されていた。[男性用かつら] [セラミックコンデンサー]事件は、小規模事業所の事例である。また、[男性用かつら]は、製品の性質上、一見の客や街頭勧誘による顧客獲得があり得ず、顧客情報が他の業種に比してことさら重要な性質を持つものであった。以上から、上記の裁判例はいずれも情報の取得者にとって秘密であることが認識できる事案であったことが決め手になっているものといえるのではなかろうか。

その種の判断を裁判所がなしているのではないかということを端的に示す例として、元取締役であるという被告らの地位に着目して情報の重要性を認識可能である旨言及するなど、秘密管理性を当該情報の利用者との関係で判断したと考えられる[ハンドハンズ]事件の判旨をみてみよう。

[ハンドハンズ]事件判決は、「秘密管理性の要件を満たすため、すなわち営業秘密として管理されているというためには、当該情報にアクセスした者に当該情報が営業秘密であることを認識できるようにしていること、当該情報にアクセスできる者が制限されていることが必要である」と一般論を述べた上で、以下のように判示した。

「スタッフカード原本は紙を綴るファイルに綴られて３つに分類されて保管されていたものであり、このうち派遣先事業所に派遣中の派遣スタッフのものは営業課の営業事務職が保管し、即時ないし近日中に就労可能な派遣スタッフのものは人材開発課のコーディネータが机の中に入れて保管し、当面就労の可能性のない派遣スタッフのものはキャビネットに収納されていたとのであり、これらは秘密として管理されていたものと認めることができる。

これらのスタッフカードについては、利用の必要のある都度、コーディネータあるいは営業課員により複写機でコピーが作成されて、営業課員がこれを持ち歩くこともあったというのであるが、これらのコピーの作成とその利用は、スタッフカードのうちの数名分について一時的に行うものであって、多人数分のコピーが同時に作成されるものではなく、また営業課員がこれらのコピーを保有し続けることは予定されていなかったものであって、業務の必要上やむを得ない利用形態と認めることができる。また、

営業課員が自分の手帳等に自己の担当する派遣スタッフや派遣先事業所に関する情報を転記して携帯していたことも認められるが、これらも派遣スタッフや派遣先事業所の一部についての情報を一時的に転記するものにすぎず、営業課員の業務の内容に照らせば、その必要上やむを得ない利用形態と認められる。他方、…原告会社では、派遣スタッフや派遣先事業所の情報の重要性やこれらを漏洩してはならないことを研修等を通じて従業員に周知させていたうえ、該当部署の従業員一般との間に秘密保持契約を締結して秘密の保持に留意していたものである。なお、被告Ｂ及び被告Ａは、誓約書を差し入れていないが、他の従業員との間に秘密保持契約を締結した当時、被告Ｂら両名は既に取締役であったためにたまたま誓約書を差し入れていないというにすぎず、上記情報の重要さについては一般の従業員以上に知悉していたというべきであるから、このことをもって秘密として管理されていないとはいえない。」

この事件は、情報を記載したスタッフカードに部外秘等の表示がなく、保管場所に施錠はなかったことから、前述の『営業秘密管理指針改訂版』によると〔情報の区分と表示〕、〔アクセス制限〕、〔施設等の管理〕に欠けるところがあったといえる事案であった。また、情報のコピーや手帳への転記が一時的にあったこと、原告がコピーや手帳の返還を求めていたという事情は認定されていないことからは、同じく指針によれば〔媒体の保管と廃棄〕に欠けるところがあったといえよう。しかしながら、判決は、情報に対して事実上アクセスが困難であると認め、また、情報の一時的な持ち出しは業務の必要上やむを得ないものであると認定し、秘密管理性の要件を満たすと判断した。

さて、本件と同様に手帳による情報の持ち出しができた事案であったにもかかわらず、秘密管理性を肯定した裁判例として、他にも先に紹介した[開成教育セミナー]事件がある。そこでは業務上の必要を超えて情報を使用することが認められていたとはいえないとして秘密管理性が肯定されていた。[ハンドハンズ]事件および[開成教育セミナー]事件のいずれの判決においても、手帳、手控えの返還、情報の抹消が求められたという事実認定がなされているわけではない。それにもかかわらず、上記のように説示して秘密管理性を肯定した裁判所の価値判断には、上記２件の事例では、業務以外には使わないという内在的な規範をもって当事者が規律されていたことで、情報の取得者は物理的な管理を要しなくても通常は情報を流用しないであろうという評価が含まれているものと思われる。当事者の主観を通じた管理がなされていたということで秘密管理性が肯定された事案であるということができよう。加えて、[開成教育セミナー][ハンドハンズ]の上記説示は、社員規模から情報への日常的なアクセスを制限できないとした[セラミックコンデンサー]と同様、業務上の効率性を考慮に入れたものであるとも推測される。

(b)秘密管理性が否定された例

ところが、近時、これらの事件と同等かそれ以上の秘密管理がされており、当事者が秘密であると認識できると推察される事案にもかかわらず、上述のように秘密管理性を当該情報の利用者との関係で相対的に判断するのではなく、物理的管理を厳格に要求し秘密管理性を結論として否定する裁判例が頻出している。これらの裁判例を子細に検討すると、そこには、秘密管理の要求水準に関し裁判例の転換があると評価せざるを得ないものがあることがわかる。以下、敷衍する。

その嚆矢となった判決として、人工歯の原型について、研究開発部主任であった被告が原型を持ち出した蓋然性は高いと推認できるとして不正利用行為を認めながらも、保管場所が各担当者の任意に委ねられ、置く場所も机の上、ロッカーとまちまちであり、収納する入れ物に部外秘の表示もなく、外部の専門家に預ける際にも秘密保持契約が締結されていないことから、客観的に認識しうる秘密管理がなされていたとはいえないとした例がある（京都地判平13・11・1判不競1250ノ174ノ22頁［人工歯］[19]）。同判決は、一般論として秘密として管理されているといえるためには「当該情報の保有者が秘密に管理する意思を有しているのみではなく、これが外部者及び従業員にとって客観的に認識できる程度に管理が行われている必要があるというべきである」と述べる。

この事件は[フッ素樹脂シートの溶接技術]と同様、秘密情報が有体物の形で存在した例であり、物理的管理体制の面では、秘密情報であることの表示、施錠、入退室制限がなかったなど[フッ素樹脂シートの溶接技術]と

[19] 小嶋崇弘「人工歯・判批」知的財産法政策学研究14号（2007年）。

共通点があるにもかかわらず、結論を異にしている。前述の[ハンドハンズ]事件が秘密情報の表示、アクセス制限、情報媒体の保管と廃棄の取り決めを欠いているにもかかわらず、当該情報の取得者の地位に鑑み相対的な認識可能性を根拠に秘密管理性を肯定しているのとは対照的である。

また、[人工歯]事件と同様に「客観的」な秘密管理性を要求するものとして、原告が製造する昇降機の販売先および販売金額に関する情報につき、秘密の表示もなく持ち出しの監視もなかったという事案で、情報が守秘義務を課された販売担当者にのみ開示されていたとしても、営業責任者である被告の仕事上の経験から営業秘密であることを当然認識できたはずというだけでは不十分であるとして秘密管理性を否定した判決（名古屋地判平11・11・17平成10(ワ)3311[コンベヤーライン]）、派遣従業員に関する情報がキャビネットに収納されていて、社員であれば誰でも閲覧可能であった事案で、元営業課長による情報の持ち出しが問題となった場合において、誓約書及び就業規則で守秘義務が課せられていたにもかかわらず、本件情報が秘密として管理されているといえるためには、人材派遣業において本件情報が極めて重要であり、性質上「機密」に該当するだけでは足りず、原告が現実に本件情報が「機密」にあたることを客観的に認識できるように管理しておく必要があるとして、秘密管理性を否定した判決（大阪地判平12・7・25平成11(ワ)933[人材派遣業社員名簿一審]）がある[20]。

さらに、相対的に言えばより高水準の管理がなされているにもかかわらず高度の秘密管理性を要求する近時の例として、元取締役らが競業会社を設立した事案につき、取締役および従業員には秘密保持義務が課されており、部屋の入り口に「関係者以外立入禁止」等の記載があり、キャビネットには「持ち出しはダメ」等の貼り紙があったにもかかわらず、キャビネット自体には施錠されておらず、秘密の表示もなく、原告従業員は入退室について特段の制限を受けていなかったとして、秘密管理性を否定した判決（大阪高判平17・6・21平成16(ネ)3846[高周波電源装置]）がある。また、顧客リスト及び登録アルバイト員の情報のリストが「持ち出し厳禁」、「社外秘」の表示のある引き出しに収められていたにもかかわらず、情報が従業員全員に閲覧可能なパソコンに保存され、パスワード管理等がなされておらず、紙媒体の情報についても回収指示や情報開示を禁止する約定はなかったとして、秘密管理性を否定した判決がある（東京地判平16・4・13平成15(ワ)10721[ノックスエンタテイメント]）。

中でも特に前述した[ハンドハンズ]事件と対称性を示すものとして[ノックスエンタテイメント]事件を紹介しよう。この事件では、原告は、コンサートや各種イベントの企画・制作等を業務とする会社であり、被告ら退職前の従業員は4名であった。被告らは元原告の従業員またはアルバイト員であったが、原告を退職した後、競業会社を設立し競業を開始し、在職中に得た情報を使用したことが問題となった。

この事件で、裁判所は、秘密管理性要件について、「情報が営業秘密として管理されているか否かは、具体的事情に即して判断されるものであり、例えば、当該情報にアクセスした者に当該情報が営業秘密であることを認識できるようにしていること及び当該情報にアクセスできる者が制限されていることなどといった事情や、パソコン内の情報を開示した場合はこれを消去させ、又は印刷物であればこれを回収し、当該情報を第三者に漏洩することを厳格に禁止するなどの措置を執ることなどといった事情がある場合には、当該情報が客観的に秘密として管理されているということができる」とした上で、以下のように判示した。

「登録アルバイト員の住所及び経歴は、登録アルバイト員リストに転記されていないところ…、履歴書及び登録表がつづられたファイルの背表紙には、赤文字で「社外秘」と記載されている。しかしながら、当該ファイルが保管されている書棚には扉がなく、当該ファイルにアクセスする者を一定の者に制限するといった措置も執られておらず、従業員が自由に閲覧できるものであったことは、前記(2)キ認定のとおりである。原告事務所には、原告代表者及び従業員を併せて4名という極めて少人数の社員が勤務しているため、業務時間中書棚に鍵をかけたり、上記ファイルにアクセスする者を一定の者に制限することは業務の円滑な遂行の観点から困難であるとしても、かかる状況下において、例えば、就業規則で定めたり、又は誓約書を提出させる等の方法により従業員との間で厳格な秘密保持の

[20] ただし、本件の二審では、本件情報がオフコンで集中管理され、キャビネットも施錠管理されていた上、守秘義務も課されていたとして、一審の事実認定を変更し、秘密管理性を肯定した（大阪高判平14・10・11平成12(ネ)2913[人材派遣業社員名簿二審]）。

約定を定めるなどの措置や、例えば、コピーを取る場合に配布部数を確認したり、使用後そのコピーを回収する等の方法により用途を厳格に制限するなどの措置を執ることは十分可能であるにもかかわらず、原告がそのような措置を執っていなかったことは、前記…認定のとおりである。以上によれば、本件においては、原告が履歴書及び登録表に記載された本件情報③を客観的に秘密として管理していたということはできない。」

この事件は退職時に従業員の手元にあった情報を回収していない点で、前述の[ハンドハンズ]事件と共通性がある。[ハンドハンズ]事件の考え方をあてはめると、本件では社外秘の印があり従業員の間で秘密であると十分認識可能であるから、退職後の情報の持ち出しは業務上予定されていないとして秘密管理性を否定しなかったのではあるまいか。この点で、[ハンドハンズ]事件と[ノックスエンタテイメント]事件は好対照である。さらに、施錠せず情報を保管していた点については[男性用かつら]事件と共通性がある。また、従業員が少数である点は、[男性用かつら][セラミックコンデンサー]事件と共通している。それにもかかわらず厳密な秘密管理を要求し秘密管理性を否定した点で[ノックスエンタテイメント]事件は注目に値する事例である。

(4) 小括

以上に見たように、秘密管理性に関する裁判例の傾向は2つに分かれていると評すべきであるにもかかわらず、『営業秘密管理指針改訂版』は、秘密として管理しているといえるための「ミニマムの水準」を過去の裁判例の分析から示したものだとされる[21]。そこには、裁判例が分かれているという認識は、垣間見ることすらできない。

その原因を探るために、『営業秘密管理指針改訂版』で引用されている裁判例を吟味してみると、同指針が依拠する裁判例のなかには、第一に、そもそも高度の秘密管理体制が敷かれているので秘密管理性要件が肯定されることに問題がない事例があることがわかる（前掲[中国野菜][作務衣][美術工芸品]など）。これらの事件では、いずれにせよ秘密管理性が肯定されているのだから、そこで挙げ連ねられている秘密管理体制に関する

[21] 経済産業省知的財産政策室・前掲注2、22頁。

事情が判文内で秘密管理を肯定する方向に参酌されているのだとしても、それらの事情がなかったとすれば秘密管理性が否定されるという判断までをも裁判所が示したということはできないはずである。その意味では、これらの裁判例が認定している秘密管理の事情をもって秘密管理性の要件が要求する「ミニマムの水準」であると捉えるのは、少なくとも誤導的であるということができよう。

第二に、従来の裁判例のうち、同種の事案で、相対的な認識可能性をもとに秘密管理性を肯定した裁判例は、秘密の印の押印（[男性用かつら]）[22]、秘密保持義務の周知（[ハンドハンズ]）[23]、コンピュータによる管理（[セラミックコンデンサー]）[24]など、指針に親和的な要素のみがピックアップされているに止まる。しかし、これらの事例では、たとえば[男性用かつら]事件では保管場所の施錠がなく、[ハンドハンズ]事件では、秘密の表示、媒体の施錠管理、持ち出しの制限および廃棄指示がなく、[セラミックコンデンサー]事件では秘密情報の表示や入退室制限がなかった、というように、指針の要求する秘密管理の水準を満たしていないというところがあったのである。そうした事情を顧慮することなく、都合のよい事情のみを抜き出したのでは、裁判例のなかから「ミニマムの水準」を抽出したということができないことは明らかである。

他方で、第三に、同指針は、[高周波電源装置][ノックスエンタテイメント]など、本稿が従来の裁判例の分析で示したように、結論が分かれうるような事例で高度な秘密管理性を要求した最近の裁判例を持ち出している[25]。たしかに、秘密の表示、施錠管理がなかった[人工歯][コンベヤー

[22] 経済産業省知的財産政策室・前掲注2、27頁。

[23] 経済産業省知的財産政策室・前掲注2、38頁。

[24] 経済産業省知的財産政策室・前掲注2、34頁。

[25] 経済産業省知的財産政策室・前掲注2、25頁。Aについてはアクセス権者の限定、施錠されている保管室への保管、事務所内への外部者の入室の禁止、電子データの複製等の制限、コンピュータへの外部者のアクセスの防止措置、システムの外部ネットワークからの遮断、Bについては「秘」の印の押印、社員が秘密管理の責務を認知するための教育の実施、就業規則における秘密保持義務についての明確な規定、誓約書や秘密保持契約による責務の設定、Cについては、情報の扱いに関する上位者の判断を求めるシステムの存在、外部からのアクセスに関する応答に関する周到

ライン][人材派遣名簿一審]は、〔情報の区分と表示〕、〔媒体の保管と廃棄〕を欠いており、パスワード管理、施錠管理がなかった[ノックスエンタテイメント]は同指針の〔アクセス制限〕、〔媒体の保管と廃棄〕がなく、施錠管理、立ち入り制限がなかった[高周波電源装置]事件は〔アクセス制限〕、〔媒体の保管と廃棄〕、〔施設等の管理〕を欠いていたといえよう。この点で、秘密管理性を否定したことは指針に適合的であった。

以上のように、『営業秘密管理指針改訂版』は裁判例のミニマムの水準を示すものではなく、一方の極の裁判例に依拠するもの、換言すれば、秘密管理の要求水準を、高度な「客観的」基準としてとらえるものといえよう。しかし、既にみたように、裁判例にはもう一つの流れ、すなわち、秘密管理の要求水準を利用者の認識に応じて相対的に捉えるものがあり、むしろ、そちらのほうがつい最近までは多数を占めていたのである。

四　検討

（一）問題の所在

以上の分析から、施錠がない等、管理に一部欠けているところがあるため、誰の目から見ても秘密であることが明らかであるとはいえないが、情報の利用者にとっては秘密であると認識しうるような場合に、裁判例は、秘密管理性を肯定するものと否定するものに分かれていることがわかった。前者は、秘密管理性を情報に接した者について相対的に判断するものであり、後者は絶対的な基準として高度な秘密管理を要求するものであるといえよう。もっとも、 近時は後者の流れの裁判例が続いており、高度な物理的管理を要するとする裁判例が有力になりつつある。『営業秘密管理指針改訂版』もこの立場に立つものである。

それでは、このような裁判例の転換、あるいは『営業秘密管理指針改訂版』の立場は正当なものといえるのだろうか。以下、検討してみよう。

（二）営業秘密制度の趣旨

まずは前提問題として、なぜ秘密管理性が要求されているのか、その趣旨を今一度検討してみよう。

わが国の不正競争防止法の沿革からは、営業秘密を保護する趣旨は、「工業上又は商業上の公正な慣習に反する」からであると位置づけられる[26]。この「公正」の意味内容が重要であり、「公正な慣習に反する」というのは、具体化すると、他人の開発投資の成果へのフリー・ライド行為を放置すると、フリー・ライドをなす者の方が有利となるとすれば、技術革新への投資意欲を低下させて産業の発達を阻害するばかりでなく、健全な自由競争秩序をも破壊し、多大な社会的損失をもたらすおそれがあるということである[27]。

すなわち、営業秘密を不正利用行為から保護する趣旨は、成果開発のインセンティブを保障するために、営業活動上の情報を秘密にすることで他の競業者に対し優位に立とうとする企業の行動を法的に支援するというところにある[28]。

それでは、このインセンティブ論の立場に立った場合、法が保護の要件として秘密管理性を要求するのはなぜなのであろうか。まず第一に、秘密として管理されていないような情報は遅かれ早かれ他に知られるところとなり、企業の優位性は失われることになる。秘密として管理していないものはインセンティブとして機能していない可能性がある。そのようなものについては、あえて法が裁判等のコストをかけて保護する必要はないであろう。したがって法的保護を欲する者には、情報を秘密として管理する相応の自助努力を促す必要がある[29]。第二に、くわえて、情報というものは管理していない場合には自由に流通する性質を有し、また形態すら当初のものを保持することなく、諸々の情報が混入して出回ることになり、そ

な手順の設定などを判断の材料としているとする。

[26] 通商産業省知的財産政策室・前掲注10、30頁。

[27] 鎌田薫「『財産的情報』の保護と差止請求権(1)」Law&Technology 7号15頁(1990年)。田村・前掲注8、18頁。

[28] 田村・前掲注8、328頁。

[29] 山口厚「企業秘密の保護」ジュリスト852号51頁(1986年)、中山信弘「営業秘密の保護の必要性と問題点」ジュリスト962号15-16頁(1990年)参照。なお、ドイツ法の概念をもとに「秘密保持の意思」を要求するものとして小野昌延『営業秘密の保護』（有信堂・1965年）536頁。

の出所源が不明となる場合が少なくない[30]。したがって、保護されるべき情報を他の情報と区別して法的保護を欲していることを明示させる必要がある[31]。

（三）趣旨に即した要請

このうち、第一の観点からは相応の自助努力がなされていなければならないということまでは導くことができる。もっとも、まさに完全に自助努力により秘密管理を貫徹することが困難であるからこそ、法は営業秘密を保護しているのである[32]。したがって、完璧な秘密管理性を要求することは、営業秘密制度の趣旨に悖ることになりかねない。さらにいえば、高度な秘密管理を要求することは、かえって企業活動に対して硬直的な効果をもたらす可能性がある。すなわち、保護されるためにそれほど高度な管理を要するなら、企業のほうは、むしろ秘密とすることを当てにして成果を開発することは断念してしまいかねない。仮にそうなってしまうとすると、秘密管理による成果開発のインセンティブを過度に減じかねないといえるだろう。

他方で、第二の観点からは、秘密情報の明示化が要請される。この趣旨を突き詰めていくと、秘密管理性は、情報の利用者にとって秘密であることがわかれば足りることになろう。すなわち、秘密管理性要件が設けられた趣旨を、情報の利用者に対して保護されている情報の識別を容易にするところに求めると、秘密であると認識できる程度に管理されているか否かを基準とすべきとする見解に結びつく[33]。この見解からは、[ノックスエンタテイメント]に代表されるような最近の高度の秘密管理を要求する裁判例の流れではなくむしろかつての[ハンドハンズ]事件のような、情報の取得者の認識可能性を基準とする立場が支持されよう[34]。

[30] 田村・前掲注8、328頁。
[31] 鎌田・前掲注9、24-25頁。
[32] 田村・前掲注8、326頁。
[33] 田村・前掲注8、329頁。
[34] 他方、情報の利用者にとっての認識を基準とする場合、公平の問題が生じうる。すなわち、[ハンドハンズ]事件のように、当該情報の重要性を認識している役職者等の上部の人間が、同じ組織内において、秘密管理についてより重い負担を強いられることは、妥当であろうか。しかしながら、役職者等は、通常、営業秘密以外の事項についても、職責上様々な権限と、同時に義務を負っているものであり、相応の対価を得ている者である。競業避止義務違反の裁判例では、役員や幹部職員についてより厳しい判断がされており(最二小判平12・6・16労働判例784号16頁[日本コンベンションサービス]など)、その類推から、相対的に秘密として認識可能な役職者等について、秘密管理性を肯定する方向に斟酌することは酷とまではいえないであろう。
[35] 小松一雄編『不正競業訴訟の実務』[中平健]（新日本法規・2006年）344頁。

結論として、上記二つの観点に立脚して最近の裁判例の傾向を肯定的に評価することは困難というべきであろう。

（四）紛争予防機能

もっとも、第三の観点として、秘密管理という要件が要求されている趣旨に、事前の紛争予防機能というものを読み込む立場が主張されるかもしれない。厳重に秘密が管理されていればいるほど、秘密の漏知行為の数も減り、裁判所をわずらわせることもなくなる。そうした紛争を予防する機能を果たすことが、秘密管理要件に期待されていると考える立場である。

この紛争予防機能を強調していけば、人工歯事件に始まる一連の裁判例に見られる秘密管理厳重化の動きを正当化することができるかもしれない。『営業秘密管理指針改訂版』も、従来の裁判例の分析からは結論が分かれうるような事例に属する[高周波電源装置]事件、[ノックスエンタテイメント]事件の事例を基準として挙げており、高度な秘密管理基準を要求しているのであるが、その背後には企業に対して秘密管理の指針を提供するという同指針の性質上、内在的に紛争を未然に防ぐという考慮が強く働いていることの現れであるかもしれない。『営業秘密管理指針改訂版』が、従来の企業における営業秘密の管理方法に関する指針に、秘密保持契約のあり方を加えたのもこの趣旨であると見ることができるかもしれない。

しかし、過去の裁判例の事案を子細に吟味すれば、そのほとんどが内部者による不正取得が問題となったものであることがわかる[35]。こうした内部者に裏切られている事例では、いかに秘密を厳格に管理しても、紛争が

起こりうることを防ぎえない。まさに秘密の利用者であって保管場所やパスワード等を知らされなければならない者(たとえば、設計業務担当者[ジーティー・ジャパン]、開発主任[人工歯]など)や、秘密を管理する責任を果たすべき者自身(たとえば支店長[男性用かつら]、営業課長[人材派遣業社員名簿]、次長[美術工芸品]など)が裏切ってしまうからである[36]。『営業秘密管理指針改訂版』は省庁が紛争予防のために策定したガイドラインであるから、企業の自助努力を促す高度な基準を掲げることは是認しうるが、既に紛争が表面化している裁判の局面でとりうる基準として、厳格な絶対的基準が望ましいかどうかは疑問である。

（五）効率性の観点

このように紛争予防機能を強化するために、秘密管理の水準を上げたとしても、大した効果が望めない反面、事務の効率化という点に鑑みると、厳重な秘密管理は日常業務に支障を生じさせかねないという弊害があることも指摘することができる。

たとえば、[ノックスエンタテイメント]事件のように従業員が４名の職場において、いちいち書類を施錠管理したり、パソコンをパスワード管理することは、業務の実態に照らして、過剰な負担を課すことになるのではなかろうか。このような小規模企業や、大企業であっても開発研究部門の従業員が数名から数十名である場合においては、全員にとってその秘密情報の重要性が認識可能であり、また、小規模企業では、口頭で注意を行うことによって、従業員間で営業秘密に関する認識を共有することも可能である。思うに、小規模企業のメリットは、大企業とは異なり、事務の簡略化や組織の簡素化を可能とするところにあるところ、大企業と同様の厳格な秘密管理を要求することは、小規模企業のこうしたメリットを減殺することになろう[37]。

[36] それを防ぐために相互のチェック体制などを強化してしまうと、つぎに述べる業務の効率性が著しく阻害されることになるだろう。

[37] 小嶋崇弘・前掲注19。以上の論旨から小規模企業に大規模企業と同様の管理体制を要求することは市場に対する過剰な介入であるとの指摘に賛同する。

（六）結論

『営業秘密管理指針改訂版』の裁判例の分析は必ずしも正鵠を射たものではなく、施錠、持ち出し禁止などの管理などが一部なされていない事例でも、情報に接する者にとって認識可能である場合には、秘密管理されていたことを否定しない裁判例がかつては多数を占めていたのである。

もっとも、最近では、高度な絶対的な基準をとりこれらの一部を欠くだけで秘密管理性を否定する裁判例が有力になりつつある。こうしたごく最近の傾向に鑑みれば、『営業秘密管理指針改訂版』の分析もあながち間違いとはいいきれないかもしれない。

しかしながら、こうした厳格な営業秘密管理を要求する立場は、必ずしも法が秘密管理を要求している趣旨から導き出せるものということはできないものである。事前の紛争予防機能を強調することで正当化しようにも、その効果に鑑みれば疑問を覚えざるを得ず、かえって特に小規模の企業にとって業務の効率性を阻害することになりかねない。従って、情報の利用者にとって秘密であると認識可能であるか否かを基準として相対的に判断する立場が妥当であると考える。