

秘密管理性要件と営業秘密管理

瀧澤 和 子 *

Confidentiality Requirements for a Trade Secret and Its Management

Kazuko Takizawa

Abstract

In order to qualify as a trade secret, the Unfair Competition Prevention Law states that the secret must satisfy three requirements: utility, non-obviousness, and confidentiality. To affirm that an asset owner has kept the information in question secret, it is necessary to demonstrate the proper implementations of multiple basic information management practices, such as physical security measures, although no single management practice is defined as critical. Today, it is not uncommon for courts to judge on a case-by-case basis and draw their conclusions about the secrecy based in part on the company's particular environment. This paper clarifies the type of information management practices that many lawsuits call into question and other relevant and influential factors, such as the nature of the information, the company's size, and the circumstances surrounding the alleged misappropriation, along with affirmed examples and criteria. Relevant US lawsuits and the debates in favor of revisions to the Trade Secrets Management Guidelines are also discussed.

要 約

不正競争防止法の「営業秘密」として保護を受けるためには、(i) 有用性、(ii) 非公知性、(iii) 秘密管理性、の三要件を満たす必要がある。秘密管理性要件を満たすためには、単一の管理策の実施が決定的になることは少なく、物理的管理など、基本的な管理策の複合的な実施が求められる。また、原告の個別具体的な状況などを考慮して秘密管理性が判断されることも多い。本稿では、訴訟の場で多く争点となる管理策の詳細、および訴訟で考慮され得る要素——情報の性質、企業の規模や侵害態様——の観点から、過去に秘密管理性が肯定された具体例や判断基準を分析した。また、米国の判例、営業秘密管理指針とその改訂に向けた動きについても言及した。

1. 研究背景

企業活動の国際化や人材の流動化、IT 化の進展などに伴い、営業秘密漏洩が頻繁に発生するようになり、かつその規模も大規模になっている。営業秘密の不正利用に対し、訴訟を提起して法的救済措置

* 早稲田大学商学大学院総合研究所 WBS 研究センター 助手

を求める場合、被告が企業秘密を利用している証拠を入手する必要がある、不正競争防止法（以下、「不競法」とする）上の「営業秘密」に該当する必要がある¹。

不競法の規定する「営業秘密」として保護されるためには、（i）有用性（保護する価値がある情報か）、（ii）非公知性（情報が公に知られていないか）、（iii）秘密管理性（秘密として管理されているか）、という三要件をみたす必要がある。このうち、最も争点に上るのは、「秘密管理性」（不競法2条6項）である。本論文では、「秘密管理性」の判断について分析し、企業が訴訟の場で保護を受けるために必要な管理を検討する。

2. 営業秘密と秘密管理性

2.1 営業秘密とは

営業秘密の対象となり得る情報は、大別して、顧客や取引先の情報・経営戦略に関する情報等の「営業情報」と、製品設計図や組立図等の「技術情報」である。

表1 過去の営業秘密侵害訴訟で秘密と認められた情報資産の例

種別	具体例
技術情報	産業用ロボットの設計図面等、部品情報、機械効率のデータ、会員制のインターネット掲示板プログラムなど
営業情報	顧客名簿、派遣スタッフ・派遣先情報、販売・仕入価格など

（出典：著者作成）

1996（平成8年）以降、秘密管理性について争った国内判例、計50件を分析した（表2）。営業情報に関する侵害訴訟では、顧客名簿等の個人情報²が争点となった事例が圧倒的に多い。昨今では、大手教育業ベネッセからの顧客情報流出など、大規模個人情報流出事件が度々世相を騒がせ、1件の情報は安価でも、大量の顧客情報を名簿業者などに売却すると、かなりの金銭的対価を得られるという認識³が、不正実行予備軍のなかで広がっている。特に個人情報保護法施行後は、消費者の意識の高まりから、従前より個人情報が入手しづらくなり、子供や学生などの情報を中心に、個人情報が「需要」の高い情報資産の一つとなっている。名簿業者への罰則が緩く⁴、名簿ビジネスが拡大していることも事態に拍車をかけている。経営戦略に関する情報が争点となった訴訟はほとんど見られないが、こうした情報は、機密情報のなかでも、とりわけ訴訟の場で争いづらい性質を持っていること、加えて、他の情報に比べて比較的手厚い管理を実施している状況⁵が漏洩事件の減少につながっている可能性もある。

技術情報に関して特徴的なことは、アジア諸国など、海外への情報流出事例がしばしば見られることである。例えば、中国企業に営業秘密が不正開示された事例として、PCプラント図面不正開示事件【No.5】があるほか、退職者経由の技術情報流出に対し、新日鉄が韓国企業ポスコを提訴中である。

表2 秘密管理性が争点となった裁判例

No	裁判所	判決日	事件番号	事件名	秘密 管理性	争点となった情報
1	大阪地判	H25.4.11	22（ワ）7025	中古車販売顧客情報事件	○	顧客情報
2	知財高判	H24.7.4	23（ネ）10084等	投資用マンション顧客情報	○	顧客情報
3	知財高判	H24.2.29	23（ネ）10061	顧客・仕入先名簿事件	×	顧客・仕入先名簿
4	東京地判	H24.4.26	21（ワ）38627等	水門凍結防止装置事件	×	装置の施工方法
5	知財高判	H23.9.27	22（ネ）10039, 10056	ポリカーボネート樹脂製造装置図面不正開示事件	○	ポリカーボネート樹脂製造装置に関する技術情報
6	東京地判	H23.9.14	22（ワ）29497	仕入先名簿事件	×	仕入先名簿
7	大阪地判	H22.6.8	20（ワ）7756等	電話占い業顧客名簿事件	○	顧客名簿
8	東京地判	H22.3.4	20（ワ）15238	派遣エンジニア、派遣先情報事件	○	派遣スタッフ・派遣元情報
9	東京地判	H20.11.26	20（ワ）853	ダンスミュージックレコード事件	×	仕入先情報
10	大阪高判	H20.7.18	20（ネ）245	和風袋物事件	○	販売先業者名 販売価格 ／仕入価格
11	大阪地判	H20.6.12	18（ワ）5172	イープランニング事件	○	掲示板プログラム
12	名古屋地判	H20.3.13	17（ワ）3846	産業用ロボット事件	○	ロボットの設計図面等
13	東京地判	H19.12.26	18（ワ）15404	スパッタリングターゲット事件	×	スパッタリングターゲットの図面
14	大阪高判	H19.12.20	19（ネ）733	スタンドオフ事件（控訴審）	×	顧客情報 派遣スタッフ情報
15	大阪地判	H19.2.1	H17（ワ）4418	スタンドオフ事件（原審）	×	顧客情報 派遣スタッフ情報
16	東京地判	H19.6.29	18（ワ）14527等	ダイニングサービス事件	×	業務マニュアル
17	東京地判	H19.5.31	17（ワ）27477等	酒類販売顧客情報事件	×	顧客情報 見積控
18	大阪地判	H19.5.24	17（ワ）2682	水門開閉装置事件	△	○：機械効率データ 部品図 ×：組立図 強度計算に関するデータ等
19	東京地判	H18.7.25	16（ワ）25672	在宅介護事件	×	介護サービス利用者名簿
20	東京地判	H17.6.27	16（ワ）24950	中国野菜事件	○	輸入先目録 顧客目録
21	大阪地判	H17.5.24	15（ワ）7411	工業用刃物事件	×	取引先名称 営業情報
22	東京地判	H17.3.30	15（ワ）26571	データファイル事件	×	顧客工場のシステム情報
23	大阪地判	H17.3.17	16（ワ）6804	損害賠償請求事件	×	取締役会議事録
24	東京地判	H17.2.25	16（ワ）18865	営業差止等請求事件	×	薬局の薬品リスト
25	東京高判	H17.2.24	16（ネ）5334	ペットサロン事件（控訴審）	×	顧客情報

26	大阪高判	H17.2.17	16（ネ）2672	高周波電源装置事件	×	装置図面 製造技術 顧客情報
27	東京地判	H16.9.30	15（ワ）16407	ペットサロン事件（控訴審）	×	顧客情報
28	大阪地判	H16.5.20	14（ワ）3030等	受託会社昇降機保守管理等顧客台帳事件	×	顧客情報
29	東京地判	H16.5.14	15（ワ）5711	作務衣事件	○	顧客情報
30	東京地判	H16.4.13	15（ワ）10721	ノックスエンターテイメント事件	×	顧客情報 登録アルバイト員情報
31	東京高判	H15.12.25	13（ワ）26301	メディカルサイエンス事件（控訴審）	×	訪問販売会員情報
32	東京地判	H15.5.15	13（ワ）26301	メディカルサイエンス事件（原審）	×	
33	東京高判	H15. 9.29	15（ネ）1791	食品包装用ネット事件（控訴審）	△	○：在庫一覧表 仕入先住所録等 ×：取引先名簿 代理店直送先台帳 単価表 輸入執務資料等
34	東京地判	H15.3.6	12（ワ）14794等	食品包装用ネット事件（原審）	△	
35	大阪地判	H15.2.27	13（ワ）10308等	セラミックコンデンサー事件	○	設計電子データ
36	東京地判	H14.12.26	12（ワ）22457	ハンドハンズ事件（中間判決）	○	派遣スタッフ／派遣先事業所情報
37	福岡地判	H14.12.24	11（ワ）1102	半導体自動封止機械装置事件	○	半導体自動封止機械装置等の情報等
38	大阪地判	H14.9.26	13（ワ）13897	実績管理台帳事件	×	顧客情報
39	大阪地判	H14.7.18	13（ワ）6368	不正競争行為差止等請求事件	×	顧客名 ニーズ情報
40	東京地判	H14.4.23	12（ワ）15215	健康食品通信販売事件	×	顧客情報
41	京都地判	H13.11.1	11（ワ）903	人口歯事件	×	人口歯の原型（に化体した情報）
42	東京地判	H13.8.27	11（ワ）25395	消防試験事件	×	業務用の書式類等 顧客名刺類
43	東京地判	H12.12.7	11（ワ）19224	セノン事件	×	顧客の契約内容一覧及び車両変動状況表 管理車両及び運転者一覧
44	東京地判	H12.11.13	10（ワ）18253	墓石販売業者の顧客名簿事件	○	暫定顧客名簿（電話帳 抜粋 顧客情報 来山者名簿 墓石原価表 聖地使用契約書 加工図・パース
45	東京地判	H12.10.31	10（ワ）4447, 13585	放射線測定器具販売等顧客情報事件	○	顧客情報
46	大阪地判	H12.7.25	11（ワ）933	サンワコーポレーション事件	×	派遣社員／ 派遣先企業情報
47	大阪地判	H11.9.14	10（ワ）1403	会計事務所顧客名簿事件	○	顧客名簿
48	東京地判	H11.7.23	10（ワ）15960	美術工芸品顧客名簿事件	○	顧客情報

49	大阪地判	H10.12.22	5（ワ）8314	タンク事件	○	ノズルの技術
50	大阪地判	H8.4.16	6（ワ）4404	男性用かつら顧客名簿事件	○	顧客名簿

○：秘密管理性肯定 ×：秘密管理性否定 △：一部の情報資産の秘密管理性肯定、一部否定
（出典：著者作成）

2.2 秘密管理性要件

秘密管理性が認められるには、（１）情報の秘密保持のために必要な管理を実施していること（アクセス制限の存在）、（２）アクセスした者に、それが秘密であることが認識できるようにされていること（客観的認識可能性の存在）、が必要とされる⁶。

このうち、要件（２）をどう解釈するかによって、訴訟で求められる管理のレベルにも差がでてしまう。「アクセスした者に」とは、情報にアクセスした者の目から見て、秘密と認識できればよいため、不正アクセス者の属性などを考慮して、秘密であることが認識できるようにされていたか相対的に判断されることになる。一方、「客観的」な認識可能性とは、「誰の目から見ても」機密情報であることがわかるほど、明白なアクセス制限が確立されていなければならないと解釈でき、秘密管理性認定を受けるには、一律に、一定以上の情報セキュリティ・レベルが要求されると主張する研究者もいる。秘密管理性を達成するために、どちらのレベルを求めるのか、長らく議論が行われ、判例では、次項で述べる通り、時期によって主流となる判例が割れている。

2.3 これまでの裁判における秘密管理性判断の変遷

秘密管理を立証して肯定されるのは容易ではなく、経済産業省が公表する営業秘密管理指針によれば、

表３ 裁判所による秘密性判断の推移

時期	変化の主な背景		代表的な判例
（１）緩和期	2003（H15）以前	—	PW 設定が無く、アクセス可能者は１件ずつデータ抽出可能で、フロッピーに社外秘表示も無かったが、実際にデータを出力するには５段階の作業が必要で、可能なのは従業員４名に限定。極めて高い財産的価値を有する顧客情報の内容等の事情を踏まえ秘密管理性肯定（放射線測定器具事件【No.45】）
（２）厳格期	2003-2007（H15～19）頃	・紛争予防機能の重視 ・法改正による営業秘密不正行為に対する刑事罰の導入	従業員全４名の企業に対し、施錠管理やパスワード管理の不十分さを理由に秘密管理性を否定（ノックスエンターテイメント事件【No.30】）
（３）揺り戻し期	2007（H19）頃～現在	・厳格期の判例への学説および企業からの批判 ・より手厚い営業秘密保護への需要増大	無施錠の棚に保管し、電子データにアクセス権設定をしていないなど不備があったが、クレーム対応の際には責任者の了解を得て配布するなど、社内関係者に対しては秘密と認識させる措置が取られていたため、秘密管理性を肯定（水門開閉装置事件【No.18】）

（出典：田村善之（2014 a）「営業秘密の管理性要件に関する裁判例の変遷とその当否（その１）」主観的認識 vs.『客観的』管理」などをもとに著者作成）

秘密管理性を判断した判例81件のうち、秘密管理性が肯定されたものは23件に過ぎない⁷。しかし、営業秘密管理体制の一部に瑕疵があった場合、直ちに秘密管理性が否定されるとは限らない。そういった事案の裁判での取り扱いには、時代によった変遷がある⁸。大別すると、（１）保有者の情報管理に多少の瑕疵があっても、不正取得者の秘密情報の認識度が高ければ、秘密管理性を認定する「相対説」に寄った判例が多く示された、秘密管理性判断の「黎明期」、（２）関係者が秘密管理を認識しているだけでなく、一定のレベルに達した厳重なアクセス制限が求められる「客観説」に寄った、原告（企業）に厳しい認定を行った判決が多く見られる「厳格期」、（３）再度、管理に厳格さが無いにも係らず、秘密管理性を緩やかに肯定した判決に回帰する「揺り戻し期」にわけられる。

過去の訴訟で、秘密管理性が認められたのはどのような場合か、第３章で具体例について詳しく言及する。

3. 秘密管理性判断に影響する要素の検討

緩和期および近年の「揺り戻し」以降は、情報の性質、保有形態、情報資産の所有者である企業の業種や事業規模、侵害態様などの諸般の事情を考慮したうえで、個別具体的に秘密管理性を判断する事例が増えてきている⁹。自社が保護したいと考えている情報資産について、管理状況と併せて、これら要素を把握しておけば、裁判の場で、どのように秘密管理性を判断されるのか、ある程度想像することができるだろう。

3.1 管理策の実施状況

秘密管理性の有無を判断するにあたって、最も重要なのは、当該情報資産の管理状況である。判例によれば、①「物理的管理」や、②「技術的管理」のなかでも、一見、基本的とも思われる管理策の実施不足を根拠に、何度も秘密管理性が否定されている。とりわけ、「アクセス権者の特定」と「秘密区分の表示」が不十分とされることが多い¹⁰。また、教育・研修の実施によって従業員に秘密の周知・注意喚起が為されていたことが判断に影響した事例¹¹、など、③「人的管理」の実施状況が考慮された例も散見される。

表４ 秘密管理性判断において問題となる管理策の例

① 物理的管理	
◎施錠管理	◎施設への入退室制限
◎秘密区分の表示（例：マル秘表示）	
◎機密性に応じたアクセス権者の設定	
◎台帳による閲覧記録	
○媒体の持出制限	
○廃棄管理	
など	
② 技術的管理	
◎ID／パスワードの適切な運用	
◎機密性に応じたアクセス権者の設定	
◎サーバの外部ネットワークからの遮断	
など	
③ 人的管理	
○秘密保持契約の締結	
△教育や研修の実施	
△委託先管理	
など	

過去の訴訟で争点となった頻度 ◎：高 ○：中 △：中～低
（出典：経産省（2013a）『営業秘密管理指針』などをもとに著者作成）

ただし、これらの要件が満たされていなくとも、媒体持ち出しの制限¹²や、誓約書等によって対象が明確化された適切な秘密保持契約の締結がなされている場合などに、秘密管理性が認められた事例もある。どれか1つの要素が秘密管理性判断において決定的なのではなく、複数の要素を遵守することが必要となる。

組織的管理の実施状況を定量的に評価することが困難なためか、過去の判例で判断された事例は多くない¹³が、情報漏洩を防ぐ企業文化を醸成する意味という観点からは、組織的管理策の強化は最も重要であるともいえる。加えて、IPA 調査によれば、内部者による不正行為に対する効果的な抑止力の要因として、「社内システム操作の証拠が残る」、「重要な情報にアクセスした人が監視される」が1位、2位を占めている¹⁴。すなわち、情報セキュリティ管理策でいえば、アクセスログの取得・レビューおよび監視カメラによるサーバ室の監視などのモニタリングが該当する。また、ベネッセ事件など、最近の情報漏洩事件を鑑みると、スマートフォン経由での漏洩防止の徹底など、現代的電子媒体・メディアへの対応が営業秘密保護において重要であることもうかがえる。

このように、漏洩事件を抑止するためには、秘密管理性を認定されるために考慮される管理策だけでなく、追加的な管理策も含め、PDCA サイクルに沿った運用と実施が求められるのが現状である。特に、システム管理者など、広範なアクセス権限を持った従業員の不正アクセスを防止するのは難しい。本稿では、秘密管理性を確保するために必要な管理策を分析しているが、実際には、事後の法的救済だけでなく、事前防止を視野に入れて、必要なセキュリティ対策を実装する必要がある。

3.2 情報の性質

技術情報は、それが保有者の下で創作されたものであり、かつ有用性の程度の高い情報であれば、当該保有者の従業者等との関係では、秘密保持の必要性や秘密の対象となる情報の範囲が比較的明確である場合が多い。また、未だ開発途上の情報と開発の実施段階の情報というように、フェーズによって取り扱いも異なるなど、特有の困難も伴う¹⁵。従って、一般的傾向としては、基本的な物理的保護も為されていない場合を除いて¹⁶、営業情報よりも若干緩やかな管理でも秘密管理性が認められてきた¹⁷。

緩和期および「揺り戻し」以降を中心に、争点となる情報の重要性が考慮された判例が見られる。世界的に希少な技術情報（PC 樹脂製造技術事件【No.5】）や、財産的価値の高い顧客情報（男性用かつら事件【No.50】、放射性器具測定事件【No.45】）などが、その性質を考慮され、秘密管理性を肯定され

表5 情報資産の性質が秘密管理性判断に考慮された例

性質	具体例	背景
財産的価値	かつら業界における顧客情報	デリケートな情報であるため、容易に収集できない
業務上の必要性	投資用マンションを購入した顧客情報	日々の営業活動に必要
希少性	ポリカーボネート樹脂プラントに関する設計情報等	世界で8つの企業グループのみが所有し、プラント製造に不可欠な独自開発情報

（出典：著者作成）

た。また、重要な情報であるほど、部署内の共有が必要になることもあるため、営業担当者とその上司の間で共有され、休日には自宅への持ち帰りがされていたものの、秘密管理性ありと結論された判例もある（投資用マンション顧客情報事件【No.2】）。

3.3 情報の保有形態

問題となる情報が、顧客名簿や設計図等のように紙媒体で保管されている場合と、コンピュータの内部または外部の記録媒体上にCAD データや Office 文書などの電磁的情報として記録されている場合とに大別できる（後者は、更に、電磁的情報が USB やフロッピーなどの可搬媒体に保管されている場合と、各クライアント PC に保管されている場合、集中管理がなされ、サーバのみにデータがある場合などに分かれる）。IT 化の進む現代では、殆どの企業で、紙媒体と電磁的情報の双方で情報が保存されているため、両方の管理が問題になるのが原則¹⁸である。

紙媒体の場合、3.1で記載の通り、印刷配布の制限や使用後の回収指示の有無¹⁹、廃棄管理などのほか、特に、ドキュメントが秘密である旨を明記した秘密の特定、施錠保管などが重要になる。

電磁的情報の管理状況について争う場合、バイオメトリクス認証や、大規模サーバールーム、フォレンジック技術の導入など、技術的管理策の完璧さを追求すれば、要するコストに際限がなくなってしまうが、裁判官の IT リテラシーの制約などもあり、現在までのところ、パスワードの設定や可搬媒体の持ち出し禁止など、むしろ基本的ともいえる対策群の実施状況が問われる場合がほとんどである。複数の観点から見て、情報管理全体のフレームワークに大きな瑕疵が無いことが重視され、目立って先進的な技術管理を行っていなければ秘密管理性が肯定されない、ということはない。

3.4 情報の不正利用者の属性

情報を持ち出す者が外部の第三者である場合と、自社の従業員・役員など（内部者）である場合とでは、要求される管理策のレベルが異なってくる。外部者との関係では、当該情報が社屋内の見えない場所に保管されていれば、秘密管理されていると主張し得るが、従業員との関係では、それだけでは不十分で、秘密管理を従業員が認識し得るよう、施錠やサーバ上のアクセス制限など、他の管理策も実施することが必要になる。

営業秘密漏洩事件の多くが、従業員または退職者、委託先など“内部者”の犯行による²⁰。終身雇用制が崩れ、雇用の流動化が進み、企業への帰属意識の低下した現代では、技術者の引き抜きなどにより、退職者からの情報不正利用が起きやすい環境が発生している。外部者の入室禁止など、基礎的な物理的制限のみで秘密管理性が認められた例もあるが、内部者にも秘密認識を持たせていたと主張できる管理を、平素から行っておくことが求められている。第5章で述べる営業秘密管理指針の改訂版においても、その点が規定される方向にある。

3.5 情報管理主体の規模

情報管理主体の大小によって、管理が求められる程度と態様は異なる。少人数の企業²¹に対して、情

報管理の程度や態様をあまりに厳格に解すると、結論の妥当性を欠くことになる²²ため従業員に対し、当該情報が重要な企業秘密であることを口頭で注意する程度で足りるとの判決²³がある。これは、中小企業が営業秘密管理に多額の予算や専任人員を配するのは難しく²⁴、単一の管理者が広範の業務を担わざるを得ないためである。従って、中小企業では、職務分掌などが完璧ではなくとも、不正利用者がその秘密性を認識しうる状況が認められれば、必要な管理は為されていると判断される余地がある。

4. 米国の制度および日本への示唆

ここで、日本の裁判所における今後の秘密管理性判断の動向の参考として、米国の状況をみてみよう。アメリカには、統一営業秘密法（Uniform Trade Secret Act）という法律がある。現在では、大半の州が、このモデル法を採択している。同法は、営業秘密に該当するには、①非公知性、②独立した経済的価値、③秘密保持のための合理的な努力（reasonable efforts to maintain secrecy）が必要、としている（1条4項）。3つ目の要件が、日本でいう秘密管理性に相当する。

米国では、秘密保持の努力の合理性を判断するにあたって、秘密保持契約の締結状況などを確認することがもっとも多いことが、Almerink et al (2012) によって示されている²⁵。これは、契約書の内容を書面で確認できるため、客観的な判断が期待できるためである。

また、当地における代表的な判例として、Dupont 事件²⁶と Rockwell 事件²⁷がある。「子供の悪戯程度のものを防ぐために多大な費用をかけることは効率的ではない」ことを判示した Dupont 事件を筆頭に、秘密管理を要求することの利益と費用を比較衡量のうえ、事案ごとにケースバイケースで最適判断をする立場を採っており、厳格な秘密管理を要求する事例は少ない。

5. 営業秘密管理指針と秘密管理性判断

不競法の所轄官庁である経済産業省は、『営業秘密管理指針』を公開し、企業がどのように営業秘密を管理すべきか、判断指標を示そうと試行錯誤してきた。度重なる改訂によって、具体的な管理策の内容に、踏み込んだ記載が充実した点は評価できるが、技術進歩や社会的問題意識の高まりによって、情報セキュリティを確保する為の措置の選択肢が、格段に増えたこともあり、紹介されている管理方法は、あまりに多岐に渡る。

当該指針は、もともと営業秘密漏洩事件の「防止」に焦点をあてたマニュアルであるため、情報漏洩防止を一義とする管理策も併記されている。現行の指針に「高レベルセキュリティを確保する管理水準」として規定されている管理策は、中小企業などにとって、秘密管理性を確保するための負担が過大だととして、企業や経済界から、秘密管理性要件を充足するための管理策を分離してほしいという要望が——また、そもそも80頁を越す長大なボリュームの指針の簡素化を要請する声が——上がっていた。加えて、前述の通り、求められる秘密管理性のレベルを左右する「客観的認識可能性」や「アクセス制限」の定義に関しても判断に悩むという意見が多かった。

このような企業・経済界からの声に対応し、2014年秋以降、管理指針の大幅改訂に関する議論が本格化している²⁸。経済産業省産業構造審議会の直近審議会（第4回・2015年1月15日開催）では、指針の

改定案が公表された²⁹。秘密管理性に関連する改訂内容は表6の通りである。

表6 営業秘密管理指針の改訂ポイント

現行の課題	改訂内容（予定）
現行版のボリューム圧縮	判例解説や冗長な説明などを削除（p.5）
秘密管理性充足のための最低限の措置と情報セキュリティ上推奨される措置の区別	指針の内容は法的保護を受けるための最低限の水準の対策に限定し、漏洩事件の防止及び事件後に推奨される対策は、別途策定する『営業秘密保護マニュアル（仮）』に記載（p.5）
「アクセス制限」「認識可能性」の定義・関係明確化 秘密管理措置対象者の明確化	「従業員」の「認識可能性」の担保のみを基礎として秘密管理性を判断。アクセス制限は必ずしも要求されず、逆に秘密表示などを行っておらずアクセス制限しか実施していない場合でも、認識可能性が担保されれば秘密管理性は肯定され得る。（p.6-7）

出典：経済産業省（2015）「営業秘密管理指針（全部改訂案）に対する意見募集の結果について」をもとに著者作成

このように、今回の指針改訂の内容は、営業秘密漏洩に対し、より広い法的救済の道が開かれ得るものとなっている。ただ、この指針は、あくまで行政当局の発行した指針であって、裁判所に対する法的拘束力を持つものではなく、今後、訴訟の場でどれだけ新指針が参照されるかは未知数であることに留意しなければならない。

6. 結論

秘密管理性を認定されるために、社内のあらゆる知的財産を営業秘密として管理することは不可能である。リスクの洗い出し・評価のプロセスを経て、自社の中核となる営業秘密を識別し、漏洩などに備えて、不競法上の保護対象となるよう管理を行っておくことが望ましい。秘密管理性を認められるためには、特定の管理策の実施が決定的な判断要素となるわけではないため、大きな瑕疵の無いよう、求められる管理策をバランスよく実施することが重要である。

指針の改訂によって、秘密管理性がより広く認められるようになれば、重要な営業秘密の保護につながり得ることは望ましいが、一方で、秘密管理性が認められる水準を満たしただけで、情報漏洩防止に十分な対策を打ったと企業が安心してしまう状況も考えられる。差止等の法的保護の対象となり得る秘密管理措置の水準と、営業秘密漏洩事件を防止するためのあるべき秘密管理措置の水準は異なり、かつ、本来は、漏洩インシデントへの「事後対応」として法的救済措置を得るよりも、インシデントを「防止」できた方が、対策の費用対効果および顧客からの信頼維持という面で望ましいのである。秘密管理性が認められるミニマムスタンダードを満たしたうえで、秘密管理性の確保だけに留まらず、漏洩防止のための管理策が求められるのだということを改めて述べておきたい。

以上

注記：

- 1 通常は、その情報資産が、守秘義務契約書・秘密保持契約書上において秘密として保護されている「企業秘密」に該当するかという点も併せて争うことが多いが、本論文は、不競法の保護を受けるための要件についての議論のみを範疇とする。
- 2 顧客情報などの全てが個人情報保護法の定義する「個人情報」に該当するわけではなく、また、取引先情報などの企業情報は個人情報の定義には含まれない。
- 3 朝日新聞、2014年07月19日、夕刊10面。
- 4 購入元の違法行為を知らなかったと主張されれば、名簿業者を逮捕できる可能性は低いと消費者庁などが指摘している。個人情報保護法は、もともと情報を所有する企業が対象で、名簿業者は想定しておらず、個人情報を保護するには不十分という声もある。一朝日新聞、2014年07月16日、朝刊5面。
- 5 経済産業省（2009）6頁。
- 6 経産省（2013a）31頁。2015年1月現在、指針の次回改訂によって、この部分が変更される予定である（5章参照）。
- 7 前掲経産省（2013a）32頁。
- 8 田村（2014a）623-632頁、田村（2013）84-86頁、近藤（2009）159頁、津幡（2007）208頁、小泉ほか（2014）16-18頁、小嶋（2007）223-229頁など。
- 9 松村（2014）35-39頁、苗村（2002）14頁など。あまりにこの傾向が強くなると、秘密管理性に関する予測可能性が低下するとして、批判的な見解もある。（石田（2011）44頁）。
- 10 経済産業省（2009）15頁。表2に示した筆者の判例分析でも同様の傾向が見られる。
- 11 ハンドハンズ事件【No.36】。
- 12 産業用ロボット事件【No.12】、水門開閉装置事件【No.18】。
- 13 データの複製が禁止されていないことが、組織的管理の未熟とされた裁判例がある。（健康食品通信販売事件【No.40】）
- 14 IPA（2014）、30-31頁。
- 15 苗村（2012）1453-1454頁。
- 16 人口歯の原型（に化体された情報）が殆ど管理されていなかった極端な例である人口歯事件【No.41】が代表的。そのほか、保管場所への立ち入り禁止表示やサーバ上でのデータ管理は行われていたものの、従業員が実質自由に立ち入り可能で、施錠やマル秘表示も行われず、他部門の社員も情報が閲覧可能だった高周波電源装置事件【No.26】など。
- 17 フッ素樹脂ライニング事件【No.49】、前掲水門開閉装置事件【No.18】など。
- 18 食品包装用ネット事件【No.34】など。
- 19 スタンドオフ事件【No.14】など多数。
- 20 経済産業省（2013b）564頁。
- 21 中小企業庁（2014）によれば、日本では、いわゆる小規模企業が9割弱を占めている。
- 22 前掲小嶋（2007）238頁。
- 23 セラミックコンデンサー事件【No.35】や、従業員6名の企業の状況に一定の理解を示した電話占い業顧客情報事件【No.7】がある。
- 24 前掲経産省（2009）12頁では、企業規模が小さいほど各管理策の実施率が低い傾向があるという結果が出ている。
- 25 Almerink et al（2012）322頁。
- 26 *E. I Dupont drNemours & Co.,Inc. v. Rolfe Christopher et, al., 431 F.2d 1012 (5th. Cir 1970)*
- 27 *Rockwell Graphic Systems, Inc. v. DEV Industries, Inc, and Robert Fleck, 925 F.2d 174 (7th Cor. 1990)*
- 28 産業構造審議会による「知的財産分科会 営業秘密の保護・活用に関する小委員会」が2015年1月現在までに、計4回開催されている。2015年内には指針改訂が実現に至る見込みである。
- 29 パブリックコメントを反映した内容となっている。——経済産業省 産業構造審議会 知的財産分科会（2015）「営業秘密の保護・活用に関する小委員会（第4回）」配布資料「営業秘密管理指針（全部改訂案）」2015年1月15日 http://www.meti.go.jp/committee/sankoushin/chitekizaisan/eigyohimitsu/004_haifu.html

<参考文献>

朝日新聞（2014a）『ベネッセ、立て直し多難 情報保護「不十分」の声 流出2895万件』2014年09月11日、7面
朝日新聞（2014b）『「名簿、金になる」持ち出し前から 元SE 供述 ベネッセ流出』2014年07月19日、夕刊10面

朝日新聞（2014 c）『名簿ビジネス暗躍 大手のデータ 1 億件超、DM 発送や削除も ベネッセ流出の陰で』2014年 07月18日、朝刊 1 面

朝日新聞（2014 d）『名簿業者の規制強化 消費者委が提言 ベネッセ流出』2014年07月16日、朝刊 5 面

青山紘一（2008）『不正競争防止法（第 6 版）』法学書院、pp. 72-76

生田哲郎・佐野辰巳（2012）「知的財産権判例ニュース 営業秘密の秘密管理性が否定されたため、不正競争行為が認められなかった事例 [東京地方裁判所平成24.4.26判決]」『発明 =The invention』109（7）、pp. 37-39

石田晃士（2011）「現代企業法研究会 企業間取引訴訟の現代的展開（8）不正競争防止法上保護される秘密情報：「秘密管理性」要件と「示された」要件の検討」『判例タイムズ』62（23）、pp. 37-49

市川穰（2007）「知的財産権 - 不競法 不正競争防止法 2 条 6 項の営業秘密の秘密管理性について判断した事例（大阪地裁平成19.5.24判決）（判例解説）」『Lexis 判例速報』3（7）、pp. 98-102

岡伸浩（2009）「説明の技法（12）顧客名簿と営業秘密 - 秘密管理性を満たすためには何が必要か」『ビジネスロー・ジャーナル』2（4）、pp. 120-123

経済産業省（2015 a）「営業秘密管理指針（全部改訂案）に対する意見募集の結果について」2015年 1 月15日

経済産業省（2015 b）「営業秘密管理指針（全部改訂案）」『営業秘密の保護・活用に関する小委員会（第 4 回）』配布資料、2015年 1 月15日

経済産業省（2013 a）『営業秘密管理指針』（2003年制定・2013年 8 月16日最終改訂）

経済産業省（2013 b）『平成24年度 人材を通じた技術流出に関する調査研究』

経済産業省（2009）『営業秘密の管理に関するアンケート調査と裁判例調査の結果分析』

経済産業省（2003）『技術流出防止指針』（2003年制定）

経済産業省 知的財産政策室編著（2006）『企業における適切な営業秘密管理』経済産業調査会

小泉直樹ほか（2014）「座談会 営業秘密をめぐる現状と課題（特集 営業秘密 その現状と向かう先）」『ジュリスト』（1469）、pp.12-31

小嶋崇弘（2007）「営業秘密の保護と秘密管理性人口歯事件 [京都地裁平成13.11.1判決]（特集 秘密管理の要件）」『知的財産法政策学研究』（14）、pp.215-240

小松一雄（2006）『不正競争訴訟の実務』新日本書院

近藤岳（2009）「秘密管理性に関する裁判例研究—裁判例の『揺り戻し』について」『知的財産政策学研究』（25）、pp. 159-234

情報処理推進機構（IPA）（2012）「組織内部者の行為によるインシデント報告書」

白木裕一（2001）「秘密管理性の肯否の基準とその実務的対応（特集 第16回知的財産権誌上研究発表会）」『パテント』64（7）、pp. 49-56

鈴木薫（2013）「秘密管理性の判断における情報の重要性・秘密性の考慮」『パテント』66（12）、pp. 68-79

高田寛（2013）「企業における技術情報の漏洩とその防止策：人的管理を中心に（星野富一教授退職記念号）」『富大経済論集』59（2）、pp. 287-311

高田寛（2013）「Global Business Law Seminar（第61回）企業における営業秘密の管理はどうあるべきか：秘密管理性を中心に」『ビジネス・ロー・ジャーナル』6（9）、pp. 110-117

田村善之（2014 a）「営業秘密の管理性要件に関する裁判例の変遷とその当否（その 1）—主観的認識 vs. 『客観的』管理」『知財管理』64（5）、pp. 621-638

田村善之（2014 b）「営業秘密の管理性要件に関する裁判例の変遷とその当否（その 2）—主観的認識 vs. 『客観的』管理」『知財管理』64（6）、pp. 787-795

田村善之（2013）「営業秘密の不正利用行為をめぐる裁判例の動向と法的な課題」『パテント』66（6）、pp. 79-101

中小企業庁（2014）『中小企業白書』

津幡笑（2007）「営業秘密における秘密管理性要件（特集 秘密管理の要件）」『知的財産政策学研究』（14）、pp. 191-213

苗村博子（2012）「判例と実務シリーズ（No.412）営業秘密侵害事件の侵害事実の立証、秘密管理性の程度：技術流出にどう対処するか [知財高裁平成23.9.27判決]」『知財管理』62（10）、pp. 1449-1459

苗村博子（2002）『判例と実務シリーズ（288）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（東京高等裁判所 平成13年（ラ）第151号 不正競争行為差止仮処分申立却下に対する抗告事件）』知財管理 52（9）、pp. 1353-1363

奈須野太（2005）『不正競争防止法による知財防衛戦略』日本経済新聞社

牧野利秋・飯村敏明（2005）『座談会 不正競争防止法をめぐる実務的課題と理論』青林書院

松村信夫（2014）「営業秘密をめぐる判例分析：秘密管理性要件を中心として（特集 営業秘密 その現状と向かう

- 先)』『ジュリスト』(1469)、pp. 32-41
- 村尾治亮・新聞祐一郎(2010)「18の裁判例から「秘密管理性」を分析 秘密情報の保護に関する判断要素(特集 日常業務だから見落としやすい! 秘密保持契約に潜むリスク)」『ビジネスロー・ジャーナル』3(6)、pp. 46-49
- ワールド・ヒューマン・リソース情報管理実務研究会他編(2011)『営業秘密管理の実務—ノウハウ、技術、ブランド保護の実践的手法』中央経済社
- Almeling, David S. et al (2010) "A Statistical Analysis of Trade Secret Litigation in Federal Courts" *Gonzaga Law Review*, 45 (2) pp. 291-334.
- Bone, Robert G. (2010) "Trade Secrecy, Innovation, and the Requirement of Reasonable Secrecy Precautions" (in *The Law And Theory of Trade Secrecy: A Handbook of Contemporary Research* (Rochelle C. Dreyfuss and Katherine J. Strandburg, eds., Edward Elgar Press), pp. 46-75
- Budden, Michael Craig (1996) "*Protecting trade secrets under the Uniform Trade Secrets Act: Practical Advice for executives*" Quorum Books
- David W. Slaby, James C. Chapman, and Gregory P. O'Hara (1989) "Trade Secret Protection: An Analysis of the Concept Efforts Reasonable Under the Circumstances to Maintain Secrecy" *Santa Clara High Technology Law Journal*, 5 (2), pp. 321-348