論　説

営業秘密管理における実務的課題

フェアトレード委員会*

抄　録　昨今の退職者の営業秘密の漏洩，海外への技術流出等が社会的に大きな問題となり，それに対応して営業秘密に関する不正競争防止法が改正され，刑事罰の導入や罰則の強化がなされている。フェアトレード委員会では，そのような状況の中，各企業の意識，管理実態等がどのように変化しているかについて06年に知財協の会員企業891社を対象に営業秘密の管理実態に関するアンケート（以下「アンケート」という）調査を行った。今回の調査の目的は，96年に行った同様の調査結果と比較し，その間に国際的な秘密情報の漏洩，窃盗などの事件が増加しているなどの実態がある中，不正競争防止法が大きく改正されたことにより，管理方法がどの様に変わって来ているのか，又はどの様な課題があるのか企業等の管理実態について調査し，報告書を発行している。

今回，当委員会では，上記アンケート結果あるいはアンケートをまとめる段階において，営業秘密の管理方法について見出した課題･問題点について，改めて検証し，実務的な観点からその管理方法を検討した。

目　次

1．はじめに

インターネット通信，光通信の発達，IT技術の進歩等により，情報の利用に関しては非常に便利になった反面，情報の管理についてはリスクが非常に大きくなってきている。また，終身雇用制度の崩壊や派遣労働やアルバイトの増加により，ますますそのリスクが増大しているのが現状である。

営業秘密の管理は，情報の種類（顧客情報，原価計算表，販売価格リスト，製造工程，運転マニュアル，新製品情報，新企画情報，開発情報，新規用途，未公開特許出願，その他技術情報等），その媒体（サンプル，物品，USBメモリー，CD，パソコン，サーバ，人等），その移動手段（手渡し，口頭，視覚，インターネット，入退社等）が様々なことから，十分な管理を行うには多くの課題が存在する。本論文では，そ

* 2008年度　Fair Trade Committee

れらの中から実務的課題をいくつか取り上げ，その対応策を検討した。

（執筆担当：2008年度フェアトレード委員会第１小委員会，桐野，籠谷，深井，堀口，渡辺，絹見）

2． 営業秘密の組織的管理

アンケート結果によると，ほとんどの企業が何らかの形で管理担当部署や管理責任者を置いて営業秘密管理を行っており，多くの企業で，専属部署・横断的組織・管理責任者の二つ以上を同時に設置しているようである。

一方で，これらの組織が具体的にどのような管理を行っているのか，複数の組織を置いている企業では，どのように役割を分担して秘密管理を行っているのかは，このアンケート結果から窺い知ることはできない。

2. 1　専属部署等の設置

「秘密管理性」[1)]を確保するためには，「秘」表示などにより営業秘密であることを特定した上で，鍵のかかるロッカーに保管する，あるいはパスワードでアクセスを制限するといった物的・技術的管理や，営業秘密を取り扱う従業員等に営業秘密の管理に関する教育・研修を行う，又は役職員等から秘密保持に関する誓約書を徴収する，といった人的管理を，実効性のあるものとして実施することが必要である。そのためには，単にルールとしてこれらの管理方法を規定するだけではなく，継続的に管理の実施状況を確認し，役職員等の注意を喚起し，必要に応じて改善を行うことが重要である。その場合，企業規模にもよるが，営業秘密管理の推進やフォロー，教育・研修活動といった役割を担った管理担当組織（者）を置くことが効率的であり，また大企業においてはより望まれるものであると思われる。

日々の業務において扱う営業秘密の種類やそれを扱う従業員の数，営業秘密を利用する頻度やその態様等は部門によって異なる為，それを効率的に管理するためには，それぞれの部門に配属されている，その部門の業務に精通した役職員を，当該部門の営業秘密管理責任者とするのが最適である。一方で，他の情報管理システムとの整合性を取りつつ，全社的な営業秘密管理の推進や制度の見直し等を行うためには，営業秘密管理の方針や計画を策定し，その遂行を全社的に監督・統括する部署が置かれていることが望ましい。

経産省の「営業秘密管理指針」（以下「指針」という）でも，組織的管理の望ましい水準として，営業秘密管理の基本方針を文書化（規程等）して定め，それを具体的に実施するための実施計画を策定することとともに，この基本方針に則り，具体的な物理的・人的管理を行うための管理責任者を置くことが重要であると述べている。

いくつかの企業に個別にヒアリングした結果では，専属部署や横断的組織の役割は，「各部の管理状況のとりまとめ」「グループ全体の管理」「情報セキュリティ体制の構築」「全社における情報セキュリティについての活動方針等の決定」といった全社的視点からの方針策定・管理であるのに対し，管理責任者は，「秘密情報の特定」「情報持ち出し管理」「営業秘密区分（極秘・秘・社外秘等）の指定」「アクセス権者の指定」「教育の実施」といった，より日常の秘密管理の実務に近い役割を担う者として位置付けられているようであり，「指針」で示されている組織的管理の望ましい水準を意識した管理体制が構築されていることが窺われる。

（1）判例の動向

組織的管理が実施されていることは，裁判等において，秘密管理性を満たしていた，と認められるための一つの重要な要素になるであろうことは容易に想像できる。しかし，現在のとこ

ろ，実際の裁判例において，組織的管理について判示しているものは少なく，また，組織的管理に触れた判例（東京地判H11.7.23［H10(ワ)15960］や，大阪高判H14.10.11［H12(ネ)2913］）でも，管理担当部署（者）の有無が主たる判断要因となっているわけではない。

(2) まとめ

判例等において，管理担当部署（者）の有無が主たる判断要因となったケースは見受けられないが，専属の管理担当部署等による管理を継続的に実施することにより，営業秘密を取り扱う従業員の意識も高まり，個々の物的・技術的・人的管理の実施が徹底されることとなる。それにより，企業として実質的に高いレベルでの営業秘密管理が実践できることになり，ひいては，裁判等において「秘密管理性あり」と判断されることにもつながると思われる。

しかしながら，社内規程に基づき管理担当部署（者）を置いていても，それが実際に機能していなければ，「秘密として管理している」とは判断されないと考えられる。組織的管理により，継続的・実質的な管理を確保するためには，管理担当部署（者）による管理が機能しているかどうかをチェックするシステム(内部監査等)がポイントになると思われる。

3． 営業秘密の特定

アンケートのその他の回答では「事業部に一任しており，実態を把握していない。」あるいは「区分して管理はしているが，徹底した管理は行われていない」という趣旨の記述は見られるものの，９割以上の企業が営業秘密あるいは秘密情報を特定して他の情報からは区別して管理しているようである。

3. 1 特定における判断基準

そこで営業秘密の特定あるいは秘密情報の重要性のランク付けを行う際の具体的な判断基準として次の３つについて考えた。

（ｉ）情報が漏洩した場合に想定されるリスクの大きさを判断基準とする方法

リスクの大小，影響度の大小は，その情報の重要性の目安としては合理的であると考えられる。それを定量化する基準項目としては次のようなものが考えられる。

① 売上高が○○億円以上の製品に直接関連する秘密情報
② 自社製品のみならず連結子会社の製品への影響も大きい秘密情報
③ 研究開発の重点テーマの技術に関する秘密情報
④ 他社との共同開発における共有成果及び他社の開示情報

（ii）具体的な書類名でリスト化する方法

各部門により，取り扱う情報が異なるので，部門ごとに営業秘密（秘密情報）に該当すると考えられるものを，例として次のようにリスト化しておくと実行しやすいと考えられる。

① 本社部門：取締役会議資料，経営会議資料 etc.
② 研究部門：重点課題年次報告，月次報告，発明届け，発明ノート etc.
③ 生産部門：生産工程表，生産工程管理表，運転記録 etc.
④ エンジニアリング部門：生産設備配置図面 etc.
⑤ 営業部門：顧客名簿，製品別売上高 etc.

（iii）アクセスを認める社員の広狭による秘密情報のランク分け

以下は一般的なランク分けの基準である。

① 極　秘：特定の従業員及び役員以外には開示しない
② 秘　　：業務上知る必要がある部署以外には開示しない
③ 社外秘：社内の者以外には開示しない

この方法では，他社との秘密保持契約により社内においても特定の従業員及び役員のみに開示が制限される他社の秘密情報については，必然的に①極秘となってしまうが，それ以外の秘密情報については結局（ｉ）あるいは（ ii ）のような基準が必要となってくる。

ここで，秘密情報のランク分けにおいて，極秘を営業秘密として保護するのか，極秘及び秘を営業秘密として保護するのか，の方針は会社により異なると考えられる。

以上の考え方を基に，営業秘密か否かを特定するための目安となるフローの例を作成した（図１）。

3. 2　電子データの識別表示

営業秘密である旨の識別表示について，表示困難なもの（例えば，契約書原本，サーバ保管の電子データや電子メール，物理的に表示が困難な物体等）には例外的に省略しているとする企業が15.9％あった。表示困難なもののうち，電子データの情報（以下「電子情報」という）について，識別表示を行わなくても秘密管理性が認められることはないのか，裁判例の分析を通して検証を試みた。

（1）裁判例の動向

近年の裁判例（平成10年以降）を調べたところ，次のような結果となった。

① フロッピーディスクに保管している電子情報について，印刷したものに識別表示があることを理由の一つとして，情報の秘密管理性を肯定している例[2]があった。

② フロッピーディスクに保管している電子情報について，当該フロッピーディスクに識別表示が無いことを理由の一つとして，情報の秘密管理性を否定している例[3]

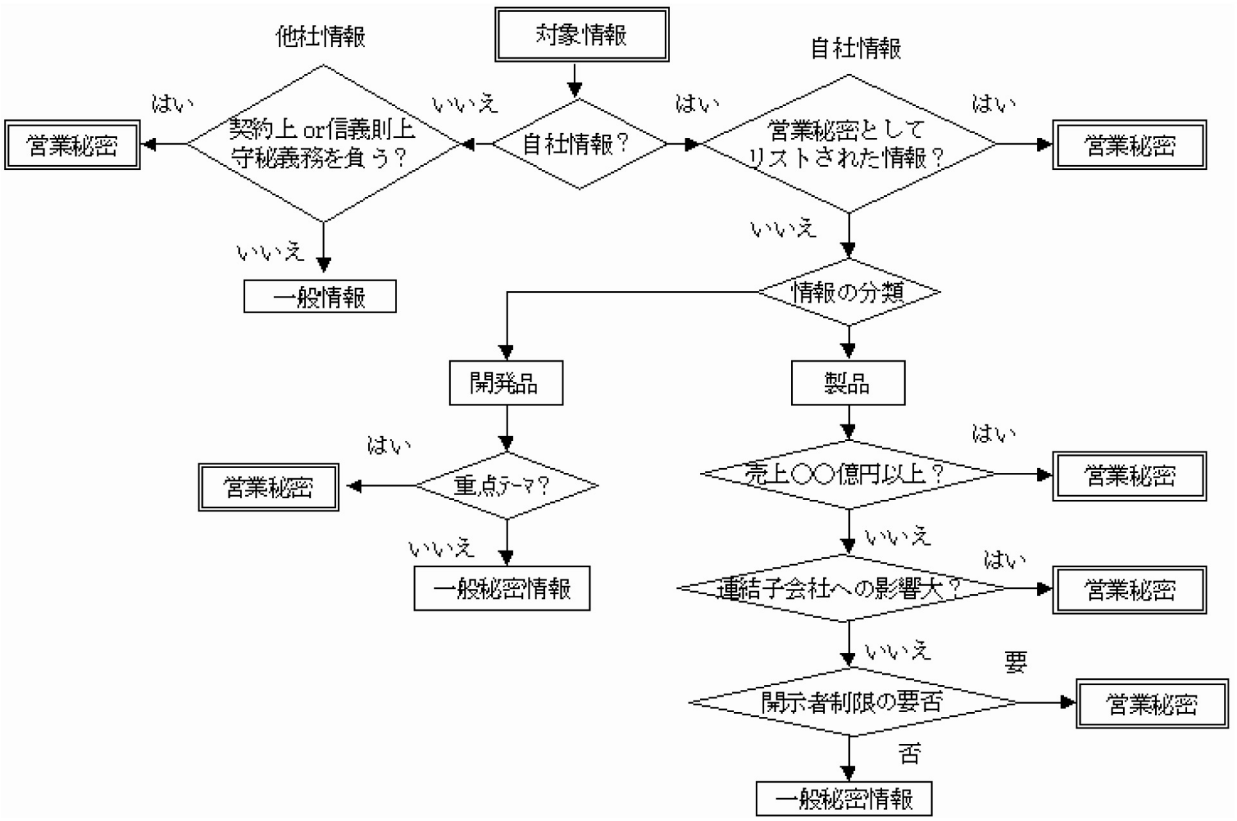

図１　営業秘密を特定するためのフロー例

があった。また，サーバ等に電子データで保管するとともに，紙媒体でも保管している情報について，紙媒体に識別表示が無いことを理由の一つとして，電子データを含めた情報の秘密管理性を否定している例[4]が見られた。

③ 一方で，コンピュータシステム上に保管している電子情報について，当該情報へのアクセス権を有する者が当該情報を格納したフロッピーディスクに識別表示が無いにもかかわらず，情報の秘密管理性を肯定した例[5]があった。また，コンピュータ上に保管している電子情報について，当該情報へのアクセス権を有する者が印刷したものに識別表示を行う取決めが無いにもかかわらず，情報の秘密管理性を肯定した例[6]が見られた。さらに，サーバに保管している電子情報について，IDパスワードによるアクセス制限があることをもって情報の秘密管理性を認めた例[7]があった。

①と②のいずれの裁判例も識別表示が単独で秘密管理性の判断の決め手になったものではない。しかしながら，電子情報をフロッピーディスクのような可搬記憶媒体や紙媒体でも保管しているような場合，③のような例があるものの，それらへの識別表示の有無が電子データを含めた情報の秘密管理性の判断に一定の影響を与えていると考えられる。

電子情報について，その電子ファイル名や格納先のフォルダ名等への識別表示の有無が，秘密管理性の有無の判断材料とされた例を見つけることはできなかった。そもそもこのような識別表示は，名称を手がかりにして営業秘密が検索（不正アクセス）されてしまうおそれもあることから，あまり推奨できない。

(2) まとめ

サーバ等で保管している電子データを可搬記憶媒体や紙媒体でも保管するような場合は，各社において識別表示のルールを制定し，それらへの識別表示を促すことは，情報の秘密管理性の確保に一定の意味があるものと考える。もちろんこのような対策だけでなく，サーバ等のIDパスワードによるアクセス管理や紙媒体を保管しているキャビネット等の施錠管理のほか，電子データの印刷制限や使用後の廃棄ルールの制定等の対策も同時に進めておくことが肝心である。

4． 物的・技術的管理

近年のデジタル化，社内web化により，企業内には大量のデジタル情報が存在し，またそれらは，従業員のPC，部内サーバ，社内の統合サーバ等に分散している状況である上に，それら情報は電子メールやUSBメモリーなどの可搬記録媒体等の利用に伴い，複製され，送信され，複製物が複数の場所に存在している状態である。このような利便性は，様々な形での情報の漏洩，企業利益の損失のリスクを増大させている。

ここでは，秘密情報の管理の内，電子データとアナログデータのそれぞれについて，「営業秘密」として法的保護要件を満たすための管理方法（管理方法１）とそれを満たしつつ効率よく無理なく漏洩を防止するための管理方法（管理方法２）を検討した。尚，社外開示，社外持ち出しを伴う運用に絡む管理方法については，ここでは含めないこととする。

4. 1 電子データの管理

(1) アンケート結果

アンケート結果によると電子データの営業秘密の管理が未実施だとする企業が全体で13.4％であり，比較的多いと言える。また，中小規模

の企業での未実施率が高い傾向がある。

（2）検討課題

管理の実施率を上げる方法がないか検討する。尚，（5）まとめで述べる通り，営業秘密としての管理が未実施であることが，即，情報管理として問題があるという訳でない。

（3）管理方法1について

アンケート結果によると中小規模の企業では営業秘密管理に係る規定類や専属部門が無いとする割合が高いことが窺える。

この原因を推測すると，中小規模の企業では営業秘密管理に係る専門部署を置く余力がないために「営業秘密」に特化した規定類を用意できていない，用意するための調査ができていないということが挙げられると思われる。

もしこの推測が外れていなければ，営業秘密の要件を満たす最低限の方法を今一度押さえることは，管理の実施率を上げることに繋がるのではないかと思われる。

要件のポイントは「秘密管理性」だが，情報にアクセスする際の制限を施すこと，アクセスする者が客観的に秘密であることを認識可能にする状態にすることであり，端的に言えば，前者はパスワード等を付した管理（必要最低限の者のみがアクセス可能な状態であること），後者は秘密の旨の表示である。

先ずパスワードについては，前記の推測以外にも，以下の事情により付与，設定していないことも考えられる。

① 設定の仕方がわからない
② 設定するとパスワードを忘れてしまう
③ 関係者に送った場合にパスワードも伝えなくてはいけないので面倒である
④ システムとして取り入れると費用がかかる

①，②は初歩的な問題ではあるが，現に存在する課題ではないかと思われる。

③，④は後述するリスクと利便性をどう考えるかの問題であり，各社，各部門によって異なって当然のことである。

ただここでは，営業秘密管理における秘密管理性を満たすことを目指し，パスワード付与，設定ありきとして検討したい。

パスワードはなるべく桁数が少ない方が利便性は高まる。2，3人のごく少数間だけでアクセスする情報であれば，パスワードは2桁でも3桁でも秘密管理性を満たすと判断されるかも知れない。但し，少なすぎてもリスクが高まり問題である。

では，秘密管理性確保のためには最低何桁程度求められるのか。ケースバイケースであって一概にはいえないものの，情報管理に関する国際規格であるISO/IEC27002においても「質の良いパスワード」は求められるが，必ずしも桁数の多いものが質がよいとされるわけではないことも鑑み，他の秘密管理策と組み合わされるのであればパスワード自体は最低4桁程度で良いのではないかと考える。こうした考えは，パスワードの桁数が少なすぎるとの理由で争いになった判例は現状においては無いと考えられること，また，金融機関等のATM取引において，カード（または生体認証）によるアクセス制限との組みあわせを前提に，暗証番号が数字4桁であること，等からもとり得ると考える。

しかしながら，パスワードの桁数については様々な議論があり[8]，将来，4桁のパスワードの有効性が問題となる可能性がある。

次に秘密の旨の表示は，その情報にアクセスする者が，その情報は企業（保有者）にとって重要な秘密であるということを認識させるための措置故，「秘」とか「秘密」などを付せば充分である。

これらのことが先ずは最低限必要なことである。勿論，これらと併せて，アクセス後の制約

（許可無く，複製させない，持ち出さないこと），一般情報と区別すること，保管場所を特定できるようにしておくこと，管理者を設けること，サーバが設置されている部屋，記録媒体の保管庫などがある場所への立入制限を設けること，社内教育を行うことがルール化されていること，HDD，メモリー等の記録媒体の廃棄時には再現不可能な状態にすることなどが追加対策として考えられるが，追加対策を行うとしても特段高い技術が必要とされるわけではないので，高い管理コストが掛かることではない。

しかしながら，表示においても次の課題はあると思われる。

①「秘」の表示は極力，表紙及び秘密情報が記録されたページのみに表示されることが望ましいこと

② 直に表示できないデータへは，間接的に表示するなどの工夫が望ましいこと

①については，例えば数百頁のWordデータの内，営業秘密は数頁しかないにも拘わらず，全頁に「秘」と表示した場合，それは全体として秘密管理性を満たさないと判断される場合もあり得るのではないかと思われる。

②については，直接書き込むことが出来ないデータベース（DB）などの電子データへの表示である。これについての工夫は，例えばメディア自体に表示する，当該DBを記録・保存するために特別に設けたフォルダに「秘」などの名称を付す，又はそのDBを動かすアプリケーションソフトが立ち上がるスタート画面に於いて，「秘」であることを表示するなどの方法が考えられる。

この様な対応は，方法によっては多少の管理コストが必要になるかも知れない。

秘密管理性を満たすには，少なくともこれらのことを社内ルールで定め，実行すればよい。このことを企業として認識すれば，営業秘密管理の実施率は上るものと考えられる。

（4）管理方法２について

次に冒頭で述べた営業秘密の要件を満たしつつ効率よく無理なく漏洩を防止するための管理について考えてみる。

「営業秘密」の要件を満たすためだけの管理とは，極論すると，漏洩が発生した後に裁判を実現させ，また有利に進めることを可能にする対策のための管理である。

企業では，この管理だけでなく，情報の物理的管理，契約，教育などを通した人の管理など漏洩を防止するためのセキュリティ度合いが高い管理が求められる。

但し，このセキュリティ度合いが高い管理の障害になるものの１つに秘密の旨の表示が挙げられる。

秘密の旨の表示は，加害者の行為に故意過失が構成されるために要求されるものであるが，表示を付すこと自体が加害者に対し，「ここに秘密情報がある」ということを教えることであって，自らリスクを高めることになるという批判がある。更には，企業内では，表示する工数が業務の円滑化の妨げになるという声も多い。

そこで考えたいことが，秘密の旨の表示無しに管理方法２を実現させることができないか，特に保管方法に注目して，検討してみたい。

秘密表示を行わずに「秘密管理性」の要件を満たすとはどういうことかというと，表示が無くても，その情報が秘密に管理され，かつ容易にアクセスできない措置が講じられていることによって，その情報は企業にとって重要な秘密情報であると加害者たる者が認識しうる状態を作ることである。例えば，パスワードの定期的変更等厳格なパスワード管理や，電子データ自体の暗号化等比較的高度なアクセス制限措置が施されていること，又は指紋認証等の生体認証で管理されていることなどが考えられる。USBメモリーのような可搬記録媒体自体の管理は，それを保管する保管庫の鍵へのアクセス

制限が厳格に行われていることが望ましい。

この考え方を有効とする判例[9]も幾つか存在する。この考え方を前提とした管理であれば，表示を要件としないため，効率よく無理なく管理することに繋がり，社内で受け入れられ易くなるのではないだろうか。

但し，管理対象の情報数が多くなると，管理コストもこれに比例するため，如何にして管理策を合理化するか，工夫が必要になると考える。

まず情報の数や種類が多い場合，専用ソフト[10]の導入または次の方法が考えられる。

各部門毎にフォルダの上位階層に，以下の内容でA，B，C各フォルダを作成する。アクセス権は，フォルダ毎に個々のパスワードで管理する（IDとパスワードでの管理だと更によい）。その下層に入るフォルダ，ファイルには関係者が必要に応じ，パスワードを付与する。この様にすれば，個々のファイルにパスワードを付与するのではなく，フォルダにあるセキュリティ機能を持たせることが必要になるが，パスワードは最低で3つ（A，B，Cフォルダ）だけ付与すればよいことになる。

A：極秘。幹部社員以上の特定の数人のみアクセス可。複製等の禁止機能，ログ機能付。

B：秘。幹部社員のみ，アクセス可。
複製等のログ機能付き。

C：普通。部員のみアクセス可

そもそも，管理対象の営業秘密が多い場合で，その一部情報が漏洩した場合，侵害の実態について，推測はできても，正確な把握は困難であることが予想される。よって，営業秘密侵害訴訟を想定して，侵害事実を正確に立証できる体制にするためには，細かなログ取得等，管理コストが嵩む可能性もある。したがって，営業秘密として管理する情報は，費用対効果を鑑みつつ厳選することが望ましいと考える。

尚，社内での流通（情報共有）をも考えると，表示に頼らざるを得ない範囲が出てくる。流通の過程で開示者から受領者に随時，「秘密情報である」と伝えるというルールでは，その過程で伝えることが不完全になりうることを考えると，営業秘密の要件を満たすとは言えないと思われるからである。

(5) まとめ

営業秘密として法的保護を受けるための管理が未実施であることが，即，情報管理として問題有りという訳ではない。例えば次のような考え方があると思われるからである。

① 業務での利便性を優先する考え方

② 重要な秘密情報については，特許権，著作権などの知的財産権としての管理に重きを置く方が有効とする考え方

③ 裁判での立証の困難性などを考慮し，「営業秘密」としてではなく，一般の秘密情報として管理するという考え方

しかしながら営業秘密が流出した場合の直接損害，及び風評，信頼低下等に伴う市場喪失等の付随的損害を考えると，法による保護は欠かせないものであり，法的保護を受けるためのルール整備やその管理を推進することは，企業にとって大変重要なことであると考える。

4. 2 アナログデータの管理

(1) アンケート結果

アンケート結果によると，アナログデータを記録した紙等のアナログ媒体の管理状況，特に社内ルールが無いとする企業が全体で18.1％であり，比較的多いと言える。また，中小規模の企業での割合が高い傾向がある。

(2) 検討課題

4．1（2）と同様に，ルールが無いことが直接，企業として問題があるという訳でないが，ルールの制定率を高められる方法がないか検討

する。

(3) 管理方法1について

アナログ媒体の管理について法律が要求する要件は4．1(3)で述べた通り，秘密の旨の表示を付した上で，施錠可能な引き出し，書棚等に施錠された状態で保管し，その鍵は必要最小限の者しか使用できないように，管理することである。

また当該アナログ媒体は，適切なルールのもと複製されること，その複製物も原本と同様の管理方法が採られることがポイントとなると考える。

これらと併せて，アナログ媒体が納められた施錠棚が設置された場所への立入制限を設けること，廃棄時には再読再現不可能な状態にすることが，その追加対策となる。

法的保護を得るためには，これらのことを社内規定で定め，履行し，繰り返し社内徹底すればよいと考えると，社内ルールの制定率は高まるのではないかと考える。

(4) 管理方法2について

アナログ媒体に記録された情報を漏洩させないためには，次のことが必要になると考える。電子データのような自由度があまり無い有体物の管理になるので，どうしても地道な管理が必要になるだろう。場合によっては，知るべき人のみが記憶する形を採り，紙媒体を作らないという管理策もあり得る。

① 原本，複製物共に，アクセス可能者，保有者を適切に制限する
② 複製物の数を必要最小限に抑える
③ 原本，複製物共に施錠管理する
④ 原本，複製物共に保有者，保管部門，保管場所をそれぞれ特定できる体制を整える（台帳化する方法もある）
⑤ 廃棄時には再読不可能な状態にする

また昨今，社内での情報のやりとりは，電子メールの本文，電子メールに添付されたエクセル，ワード，パワーポイント等のデジタルファイル，プロジェクターを用いた口頭での説明などであり，社内で使用される紙媒体の内，「営業秘密」に該当する情報が記録された紙媒体は，かなり限られている。

よって，その限られたアナログ媒体の管理さえしっかり行えば，最低限必要なリスク回避に繋がると言える。

例えば，会議の場などで配布される資料は，プロジェクターで投影されるものの，手元に同じ資料が有った方が効率がよいときなどに配布されることがある。この紙媒体自体を「営業秘密」として管理するためには，社内規定に基づいた秘密の旨の表示を付した上で，更には「営業秘密」であることを宣言し，注意喚起した上で配布し，受領した者には，社内規定で定められた管理方法を遵守させることで足りる。また漏洩を防止する為には，可能な限り会議終了後に回収することが望ましい。

また，筐体や金型などの設計図については紙で保管され使用されている場合が多い。これらについては，やはり同様に秘密の旨の表示を付した上で，施錠棚等に保管する，また使用する場合は，必要最低限の者しか見ない形で使用し，それが複製物である場合は，使用後はシュレッダーで廃棄するなど第三者が見ることがない形で廃棄すればよいと考える。

(5) まとめ

アナログ媒体については「営業秘密」の要件を満たすためには，表示と施錠は必要最低限の要件となる。不正競争防止法の「営業秘密」の要件は，個人情報保護法のように義務規定ではなく，事前に要件を満たす管理を行っていれば，漏洩時に法的保護が与えられるとするものであり，企業としてその管理を行うか否かは，要す

るに日々の利便性を採るか，リスク軽減を採るかは各企業で判断することである。しかし，本当に重要な情報に対しては，この法が与える要件を満たす管理を行えば保護するという選択肢を採用しない手はないのではないかと考える。

4. 3　電子メールの問題点

秘密管理性の有無を左右する物的・技術管理のうち「電子メールを利用した営業秘密の送受信」についてアンケート結果をもとに問題点と対応策案を検討した。

(1)「秘密管理性」に関する問題点

アンケート結果より，「電子メールを利用した営業秘密の送受信」についてルールを決めて規制を行っている企業の割合は78％であり，「営業秘密管理を定める社内規定類がある」と回答した企業の割合（95.6％）や「営業秘密が電子データである場合，アクセス制限等の対応を行っている」と回答した企業（約90%）に比べるとかなり低いと思われる。

電子メールが，今日のビジネスに必要不可欠な存在となっている中，22%の企業が全く規制を設けていないのは，営業秘密の漏洩防止等，特に「秘密管理性」の観点において次のような問題があると言えよう。

① 送信途中（ネット上）で情報搾取される可能性がある。
② 大量の営業秘密情報を容易に社外へ送信（持ち出し）可能であり，漏洩した場合の被害が莫大となりやすい。
③ 電子メールでの送信は簡便であるため，紙文書に比べ営業秘密の認識が希薄となり易く，情報の重要性を認識しないまま送信してしまう恐れがある。
④ 自己のパソコンに秘密情報が送信記録として残留し，アクセス制限の不備やデータ保管の安全性低下の恐れがある。
⑤ コンピュータウィルスやワーム等による情報漏洩の危険性が高い。
⑥ 宛名ミス，うっかり送信等の誤操作が発生しやすい。

電子メールの利用を含め，営業秘密に関する情報漏洩発生割合の７～８割は，内部者による行為・犯行とされている。企業がどんなにITを駆使し，ネットワークへのアクセス制限や認証，暗号化を強化しても，正規のアクセス権を有する内部者の犯行は簡単に防げないという問題も存在している。

(2) 対応策案

電子メール利用時の情報漏洩防止策に関して，ITによる技術的な防止策に加え，内部犯のような技術的な対策だけでは防げない問題への対応策も検討した。

（ｉ）技術的な（教育を含む）情報漏洩防止策

① 秘密情報を電子メールにて送付する際，暗号化，パスワード化を徹底させる。
② 従業員への事前教育・研修により電子化された機密文書，重要文書，一般文書等においても区分を徹底し，秘密情報にアクセスすることへの責任感を持たせる。
③ 住所録検出機能がついたメールサーバソフトで顧客情報を含む添付ファイルのフィルタリングを行い社外への送信を制限する。
④ 多重・複合圧縮された電子メールは，サーバソフトで容量毎に社外への送信を制限する。
⑤ メールサーバソフトで社外送信制限キーワード（「社外秘」，「売上」etc.）を設定し，送信制限を行う。

（ⅱ）従業員への告知による抑止策

① 従業員が社外宛てに電子メールを送付する際，必ず上長へCCを送付（もしくは自動的に送付）する。

② 全てのメールをサーバへ保存し，送受信文書の監査を行っていることを従業員へ告知し，秘密文書の社外送付を抑止する。

4. 4　営業秘密の持ち出し規制

営業秘密の管理場所外への持ち出しについては，全体の49.9％と約半数の企業が管理責任者等の許可を要件としていた。そこで，持ち出し規制の運用上の課題として，管理責任者による持ち出し許可の記録方法について考えた。

(1) 裁判の動向

近年の裁判例では，資料を持ち出す際，書面で上司等の了解を得ることとされていたことを一つの理由として，当該資料に記載された情報に秘密管理性を認めた例[11]がある。

一方で，以下のようなケースにおいても秘密管理性が認められている。

① 持ち出す際，管理台帳に持ち出し年月日や氏名等を記入することとされていた資料（管理責任者等の許可まで要求されていたかは不明）に記載された情報について，秘密管理性を認めた例[12]

② 顧客に交付する際，責任者の了解を得ることとされていた資料（了解を得た記録を残すことまで要求していたかは不明）に記載された情報について，秘密管理性を認めた例[13]

③ 職員が一部分をコピーして持ち歩いていたり，手帳に転記して携帯していたりした資料の記載された情報について，秘密管理性を認めた例[14]

これらの裁判例からすると，持ち出しの際，管理責任者の許可の記録を残すこと，さらには管理責任者の許可を得ることも秘密管理性が認められるうえで必須とは言えないと考える。

(2) 持ち出し許可の記録を残す意義と課題

持ち出しの際の記録を残すことについては上述のとおりであるが，以下の点において意義があると考える。

① 持ち出した者と許可した管理責任者を記録しておくことで，持ち出しの責任の所在を明確にできる。

② 記録を定期的にチェックすることで，持ち出し後の営業秘密の廃棄・返却漏れを防ぐことができる。

一方で，記録を残す上での課題は，記録の手間であり，特に営業秘密を頻繁に持ち出すような職場では，運用が廻らなくなるおそれがある。

(3) 記録の残し方

上記の意義を達成しつつ，課題である記録の手間を省く観点から，以下のような記録の残し方が考えられる

① 持ち出しの申請と許可を電子メールで行い，責任者が電子メールを保存しておく方法。パソコンのメールソフトに持ち出し案件の電子メールを入れておく専用フォルダを作成しておけば，電子メールを手がかりに上記(2)②のチェックを行うことも比較的楽になると考えられる。

② 社内LAN等を用いた許可・承認システムの中に持ち出し許可申請についても組み込む方法。

さらに，全ての営業秘密について持ち出し許可の記録を残すのではなく，顧客リスト等重要なものに限定して記録を残す運用とする等，各企業にあった方法・運用になるよう工夫していけばよいと考える。

(4) 記録を残す運用を担保する仕組み

持ち出し許可の記録を残す運用を導入した場合，それを担保する仕組みとしてはどのようなものが考えられるか。特に上記(2)①の観点な

どからは，持ち出し前に許可の記録を残す運用とするのであれば，記録を残さないと持ち出し手続きが進まなくなるような仕組みがあることが望ましいと考える。

営業秘密を持ち出す方法として，パソコンやUSBメモリー等の可搬記憶媒体に格納して持ち出す方法や，紙媒体で持ち出す方法，電子メールで送付する方法など様々な方法が考えられるが，それら全てについて記録を残す運用を技術的に担保する仕組みを導入することは，導入コスト等の面から容易ではないものと考えられる。記録を残すことを義務付ける内容の社内ルールを制定し，繰り返し社内教育を実施するほか，当該ルールが遵守できているか定期的に監査を実施する，社内ルールを守る旨の誓約書を取得するなど，記録を残す運用を心理的に担保する方法をまずは採用することが望ましいと考えられる。

5． 人的管理

5. 1　中途採用者の対応

アンケート結果において中途採用者から何らかの形で秘密保持誓約書を取得している企業は，68.6%，元の就職先に対し秘密保持義務を負っているかどうか確認している企業は，44.1%であった。

(1) 中途採用者の営業秘密の開示が，転職先の会社の「不正競争」行為となる場合

中途採用者が転職前に所属していた企業の秘密情報を転職先の企業に漏らした場合，転職前の企業から不正競争防止法に基づき，差止，損害賠償，信用回復措置等の請求を受ける可能性がある。他社の営業秘密を中途採用者から，営業秘密の不正取得行為や不正開示行為が介在することについて「知って」又は「重大な過失により知らないで」取得することは，「不正競争」行為に該当する。例えば，最初から競合会社の営業秘密を不正開示させる目的で競合会社から採用して自社内で開示させる行為は典型的な不正取得になる。

すなわち，中途採用者が旧勤務先の営業秘密の不正取得・開示行為等を行い，その者を通じて，「知って」又は「重大な過失により知らないで」営業秘密を取得した場合には，「不正競争」行為に該当する。したがって，中途採用者が営業秘密を不正取得していない，又は不正開示しないことにつき，確認又は保証を取っておくことがポイントになるものと考える。

(2) 具体的な実務上の運用について

実務において，転職先の会社が上述の「不正競争」行為を行ったと判断されないために具体的にどのような対応をとるのが望ましいかを検討した。

（ⅰ）採用活動時の対応

① 自社への転職を勧誘する場合には，他社の営業秘密の開示を前提とした転職を求めたり，他社従業者からの積極的な売り込みは受け入れたりしない。

② リスク回避の観点から，不正をほのめかすような者の雇入れを避ける。

（ⅱ）中途採用者の負っている義務の確認

① 会社の制度として，中途採用者に対して面談等をして，転職前の企業からどのような義務が課されているかの確認を行うことにより，中途採用者の前勤務先から営業秘密を受領し不正に使用したとして訴訟を提起された場合でも，「不正競争」行為を行っていないことを主張しやすくなる。

② 中途採用者の退職時の契約書等の秘密保持義務や競業避止義務の内容について確認できれば，中途採用者への対応が取りやすい。

③ 転職前の企業が，退職時の誓約書等の写しを退職者に交付しないため，もしくは契約書の内容を開示しない義務を課しているため，どのような義務が課せられているか確認できない場合，又はすべての情報を第三者に開示，漏洩してはならない，というような漠然とした義務を課されている場合等には，明確な秘密保持義務の内容は，転職先の会社には，わからない。この場合でも，転職先の企業は，「不正競争」行為を行っていないと主張できるような対策を取ることが望ましい。

具体的には，

（ア）転職前の企業での業務内容・秘密保持義務の内容など，採用におけるチェックリストのようなものを策定しておく。

（イ）場合によっては，転職前の企業に対して，一定の合理的な質問状を送付する。

などの対応が考えられる。

④ 転職前の企業から警告書が届いた場合には，その内容につき，中途採用者に十分に確認することが重要である。なお，転職前の会社から警告を受けた場合には，「知らないで」営業秘密を取得あるいは使用したという主張はできなくなる。

(iii) 誓約書の入手

中途採用者からは誓約書を取得する場合，以下のような項目を盛り込むと実効性のある誓約書となる。

（ア）前勤務先の営業秘密を，自社で開示又は使用しないこと

（イ）前勤務先において完成していた職務発明等を自社名義で出願しないこと

（ウ）自社の業態，自己の携わる業務に関して，競業避止義務を負っていないこと

(iv) 配属時の対応

① 面接時・入社時に，転職前の企業の営業秘密を自社内に開示・使用しないよう注意・教育をする。

② 面接時の情報を元に，入社時に，競業避止義務や秘密保持義務に十分に留意した配属先を検討する必要がある。

(5) 採用・配属後の対応

① 誓約書によってもなおリスクがあると考えられる場合には，漏洩の懸念がなくなるまでの一定期間，前職との関係性の薄い業務に従事させる等のより慎重な対応を検討する。

② 中途採用者の採用・配属後も，当該中途採用者の業務内容を定期的に確認することにより，元の会社との間の秘密保持義務違反が生じないよう確認をする。

(6) まとめ

実務上は，中途採用者が転職前の企業に対して負う義務を確認する，中途採用者から誓約書を取る，中途採用者の配属に注意する，といった対応をとるのが一般的な方法である。問題が起きた場合には中途採用者の転職前の企業に説明でき，訴訟になった場合にも「不正競争」行為をなしたと判断されることのない相応の管理を行っていることを証明できるような体制を制度として整えていくことが望ましいと考える。

5. 2 社員の教育・研修

アンケート結果によると，企業規模が大きくなるに従って，秘密情報管理又は営業秘密管理に関する教育研修制度が「ある」と回答している企業数は増えている。

秘密情報管理や営業秘密管理に関する規則や管理体制を整備しても，営業秘密を取り扱う従業員や営業秘密の管理責任者がその重要性について認識していないと，これらの規則や管理体

制も「画に描いた餅」になってしまう。従って，秘密情報管理を実効性のあるものとする為には，規則や体制の整備と併せて，従業員に対して秘密管理の重要性や管理組織の概要，具体的な秘密管理のルールについて周知徹底し，これを遵守させるための教育や指導が重要となる。

こういった教育や指導は，日常の業務における指導・監督のレベルでも可能であり，アンケート結果で「教育・研修制度がない」と回答した企業の中にも，このような日常業務レベルでの秘密管理に関する指導・注意喚起を行っている企業は相当数あるのではないかと推察される。しかしながら，部署における担当者の異動等を考慮すると，こういった日常業務レベルでの教育について継続性・一貫性を維持することは難しい。

「指針」でも，従業員に対する教育・研修の実施に関する「望ましい水準」として，「組織体制の中に教育責任者を設置する等により組織内における教育責任を明確化し，定期的教育を実質的に確保することが望ましい。」と述べられている。

(1) 教育・研修制度の内容

具体的に教育研修制度を検討するに当たっては，どのような内容の研修を，誰に対して，どれくらいの頻度で行うかがポイントとなるが，「指針」等でも明確な基準は示されておらず，各企業においてその業務態様に応じたものを検討しなければならない。

教育研修の対象者については，もちろん全社員を対象にすることが望ましいが，研究部門その他営業秘密の取り扱い頻度の高い部署の社員のみを対象にするのも一つの方法である。また，対象となる社員に応じて異なるレベル（例えば全社員には情報管理のポイント全般を，秘密情報を取り扱う部門の社員には，情報管理のより詳しいルールを，あるいは技術情報を扱う部門の秘密管理責任者には，技術流出防止に関する現状，対策，関連法規等の研修を行う等）の研修を行うのも適切であろう。

研修内容としては，営業秘密保護や不競法を意識した内容の研修を行うことが必要であるが，昨今では，営業秘密に限らず，個人情報その他の情報管理全般に対する対応が必要になっていることから，情報管理全般の研修の一部として営業秘密を取り上げるという方法も考えられる。また，研修の方法として，ｅラーニングを採用することも検討に値する。

教育研修の頻度としては，「指針」にもあるとおり，定期的に実施することが望ましい。年１回程度というのが一般的と思われるが，異動時や昇格時等の研修と合わせて行うのも一つの方法である。

(2) 判例の動向

秘密管理性について判断した判例の中には，その判断要素として「教育・研修制度」に触れている判例がいくつかある。例えば東京地判H14.12.26中間判決［H12(ワ)22457］（派遣事業を営んでいた原告会社の取締役であった被告が原告会社の営業秘密である登録派遣スタッフ及び派遣先事業所に関する情報を持ち出し，転職先の被告会社に開示した事案）では，「研修等を通じて本件情報の重要性やこれらを漏洩しないことを従業員に周知させており，該当部署の従業員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。」と述べ，秘密管理性を認めている。また，「会社の仕入先リスト，顧客先リスト，仕入マニュアル，営業マニュアルなどは会社の最も重要な営業秘密であることを認識し，十分注意して社外に持ち出すことを禁止すること」「業務上の機密に属することは在職中はもちろん，退職後も，これを会社の目的以外に使用しないこと及び他に漏洩しないこと」等を規定した就業規則を営業所内のホワイ

トボードに掲示したり，従業員に対し，毎朝行っている朝礼において，随時，新聞等に掲載された営業秘密に関する事件を紹介するなどの教育を行ったりしていた事案[15]において，秘密管理性を認めている。

しかしながら，教育・研修制度が実施されていることが決定的な要因になっているわけではなく，一通りの物的・技術的管理が実施されている場合にそれを補足・補強する要因として教育・研修制度に触れている，というのが傾向のようである。例えば，東京地判H19.10.30［H18（ワ）14569］（仮住まい物件の仲介を主たる事業とする原告会社が，原告の営業秘密である顧客情報を原告会社従業員及び取締役であった被告らが不正に持ち出し，被告会社を設立した上で被告会社の営業に上記の顧客情報を使用したと主張した事案）では，「仮に，原告が，各従業員に対し，名刺のコピー及び社外持ち出しの禁止，並びに名刺ホルダーに入れての机内管理を徹底指導していたとしても，従業員に対する情報管理指導がされていると言うに留まり，保管場所への施錠などにより，アクセスすることができる者が限定されていたことや，名刺や名刺ホルダーに秘密であることの表示がされているなど，アクセスしたものが当該名刺が秘密であることを認識することができる状態であったことについては何ら主張立証がない」として秘密管理性を否定している。

また，情報管理に関する教育・研修を実施していた場合であっても，それが営業秘密管理を意図したものでない場合には，秘密管理性の判断要因としては考慮されない可能性がある。例えば，訪問介護サービス事業を営む原告会社が，原告の従業員であった被告らが被告会社を設立し訪問介護サービス事業を営んでいることについて，被告らが原告の営業秘密である利用者名簿を不正に持ち出して使用していると主張した事案（東京地判H18.7.25［H16（ワ）25672］）では，「雇用契約上の秘密保持義務や指導教育は，利用者のプライバシー保護を念頭におくものと解するのが相当であって，これによって不正競争防止法上の営業秘密性が直ちに導かれるものではない。」と述べ，秘密管理性を否定している。

秘密管理性の判断において教育・研修の実施について触れた判例は決して多くはないが，これらの判例からは，

① 教育・研修が実施されていることは，秘密管理性の認定における一つの要素ではあるが，決定的な要素ではない。あくまでも，その他の管理手法によるアクセス制限や客観的認識可能性が一応確保されていることが前提とされている。

② 教育・研修については，必ずしも組織的なものである必要はなく，日常業務における上司等からの指導・監督といったものでもよい。重要なのは，それによって従業員等がどの情報が営業秘密であるかを認識し，かつその管理が重要であることや漏洩・不正開示を行ってはいけないことを認識できる程度のものかどうか，という点である。

③ 上記②とも関連するが，顧客の個人情報等に関しては，いわゆるプライバシー保護や個人情報保護法に関する教育・研修では，不正競争防止法上の営業秘密の要件としての秘密管理性を導くものとしては不十分であり，同法に基づく保護を念頭においた，営業秘密の管理や運用等に関する内容を含んだ教育・研修でなければならない。

といった傾向を読み取ることができる。

（3）まとめ

判例をみても，教育・研修の有無が秘密管理性の判断における決定的な要因となることはない。しかしながら，企業において物的・技術的

管理を確保するためには，営業秘密管理に関する意識が従業員等に浸透しており，それに関するルールが遵守されていることが重要で，それは従業員に対する教育・研修なくして確保することは難しい。従って，教育･研修制度については，秘密管理性の直接の判断要素としてだけではなく，主要な判断要素である物的・技術的管理の確保に間接的につながる要素として重要であると考えられる。

また，営業秘密の漏洩・不正開示は内部者によるケースが殆どである。判例では，秘密管理の一部に瑕疵があっても，内部者にとって秘密であることが認識できる状況であったことが認められれば秘密管理性があると判断しているケース（例えば，東京地判H14.12.26［H12(ワ)22457］及び大阪地判H19.5.24［H17(ワ)2682］）もあり，学説上も内部者による漏洩・不正開示の事案における秘密管理性についてはそのような相対的判断をすべきとしているものもある[16]ので，教育・研修により営業秘密に関する認識の徹底が図られているかどうかは実務上重要であると思われる。この点からも，各企業の規模や業態に応じた教育研修制度を構築することが必要だと思われる。

6． 法的管理

6. 1 新卒者，中途採用者からの秘密保持誓約書

(1) 秘密保持誓約書取得に関する問題点

アンケート結果より，新卒者，中途採用者から「秘密保持誓約書」を取得している企業の割合は約７割であった。

これは，秘密管理の意識があると判断される「営業秘密管理を定める社内規定類があるもしくは策定中」と回答した企業の割合（95.6％）と比べると，低い数字と言える。

「秘密保持誓約書」を取得しない理由として，「就業規則に盛り込まれているから十分である」や「誓約書の抑止力に有効性が感じられない」という意見もあったが，取得しない場合のリスクとして以下のことが考えられる。

① 不正競争防止法上求められる「秘密管理性」の法的要件が，不十分となる可能性がある。

② 従業員が自社の営業秘密に対し守秘義務を負っていることへの意識が希薄になる。

以下で挙げた判例を見る限り，必ずしも「秘密保持誓約書」を取得することが，不正競争防止法上の保護を受けるための要件ではないと考えるが，上記リスクを軽減する意味でも「秘密保持誓約書」を取得することは有効であると思われる。

(2) 判　例

（ⅰ）美術工芸品販売事件[17]

被告が退職する際，原告会社が保有管理している顧客名簿を持ち出してこれを原告の同業他社に売却した事件で，持ち出した顧客名簿が秘密に管理されていたかどうかを証明する証拠の一つとして，原告会社が，秘密保持義務を就業規則に定め，被告に在職中職務上知り得た顧客情報を第三者に漏らさない旨の誓約書を提出させていたことを挙げた事例。

（ⅱ）在宅介護サービス営業秘密事件[18]

裁判所は，利用者名簿について，入社時の労働契約書や被告から１年ごとに守秘義務に関する誓約書を取り付けていたことに関し秘密管理性を認めつつも，利用者名簿の実際の管理状況やアクセス制限がなかったこと等を理由に秘密管理性を否定し，最終的に不正競争防止法上の営業秘密に該当しないと判断した事例。

(3) 対応策案

上記判例より，新卒者等から誓約書を取得する効果として，「秘密管理性を証明する証拠

(法的管理力)」が挙げられる。しかし，誓約書を取得したからと言って秘密管理が十分とは言えず，随時，従業員教育や啓発により実効性を保ち，実務上十分な秘密管理がなされていないと秘密管理性は認められないこともある。

とはいえ，誓約書の取得は，不正競争防止法上秘密管理が認定される一要件となっていることから，取得することを推奨する。誓約書を入手する場合の注意点及び対応策は次の通りである。

① 入社時及び就業時には，誓約書等の秘密保持契約書を締結し，守秘義務の自覚を促す。

② プロジェクトに参加するなど当該従業員が営業秘密として管理すべき情報を知ることになった都度，新たに守秘義務の対象を特定し誓約書を締結する。

③ 誓約書を取得しない場合でも，代替措置として，就業規則等の社内規程で秘密保持義務を確保する。ただし，営業秘密の守秘義務のほか不正に取得・使用・開示するなどの従業員の行為に対し懲罰規定を設ける場合は，労働組合や従業員代表の意見を聞く必要がある。(労働基準法第90条)

6. 2　退職者からの誓約書の取得と競業避止

(1) 退職者から秘密保持誓約書を取得しない場合の問題点

アンケート結果より，一般従業員から「秘密保持誓約書」を取得している企業の割合は67.2%，役員から取得している企業は23%であった。

退職者については，退職時の会社の営業秘密を持ち出して競合企業に再就職したり，自分で起業するなど，営業秘密の漏洩や不正使用が発生する可能性が高いことから，新卒者や中途採用者より誓約書取得の重要度が高いと思われる。しかし，新卒者や中途採用者からの取得率とほとんど差がなかったというのが現状である。

「秘密保持誓約書」を取得しない理由として，「入社時の秘密保持契約書に退職後も含められている」や「役員については守秘義務を負うのが当然」という回答もあったが，「取得すべきと考えているが実行上取得できていない」という企業も18.6%に上っている。

製造拠点が海外に移り，日本企業を退職したエンジニアが海外企業で働くなど，退職者を介した情報漏洩の危険性は高まっている。それゆえに退職者に対する秘密保持誓約書の締結は重要であると言えよう。また，特に競業避止義務を課す誓約書の場合，以下の判例からわかる通り，一律的な誓約書ではなく，対象となる情報を特定し競業避止期間を設ける等の個別の対応が望ましい。

(2) 判　例

(ⅰ) 岩城硝子事件[19]

在職中に取得した誓約書による競業避止の合意は,その対象について非常に広範であること，場所的限定がないこと，期間（5年間）が長期に過ぎること，代償措置がないことが不十分であることを理由に，競業避止義務を無効とした事例。

(ⅱ) ダイオーズサービシーズ事件[20]

競業避止義務を課した誓約書の内容が，「退職後2年間，在職時に担当した営業地域やその隣接地域にある同業他社に就職をして，あるいは同地域にて同業の事業を起こして，貴社の顧客に対して営業活動を行ったり，代替したりしないこと。」となっており，裁判所が，期間，区域，職種，使用者の利益の程度，労働者の不利益の程度，労働者への代償の有無等が合理的な制限の範囲であると認めた事例。

(3) 提案・対応策

退職時の誓約書取得については，アンケート

結果より次のような対応が考えられる。

① 退職者については管理職のみ誓約書を提出させる。
② 入社時に職務発明の承継に関する誓約を兼ねて全員から誓約書を取得する。
③ 社内規程で，管理責任者は必要に応じて誓約書を提出させることができる。
④ 対象者，部門により取得するかを個別に判断する。
⑤ 誓約書を提出させる対象者を限定し，守秘義務範囲を明確化させるために「退職前10年間に従事した業務を退職者自身に書かせ，退職者にとっては詳細に書けば書くほど守秘義務の範囲が狭まる」という意欲付けを行う。

特に，競業避止義務を課す場合，上記判例に見られる通り，競業避止の合理性を求められるのが通説であり，合理性の判断要素としては，（ア）競業避止義務の目的（使用者の正当な秘密・ノウハウの保護など），（イ）労働者の在職中における地位・職務，（ウ）競業禁止の範囲（職種・場所・期間）及び（エ）代償措置の有無・内容などが挙げられる。

全ての退職者から詳細な秘密保持誓約書を入手するのは困難ではあるが，少なくとも重要度の高い営業秘密を扱う部署の退職者から詳細な誓約書を入手することが望ましいと考える。

また，役員については，会社法上，在職中は会社に対する忠実義務（会社法355条），競業避止義務（会社法356条１項）を負っている。しかし，退職後も秘密保持義務を負っているとは必ずしも言えないため，従業員の退職と同様，役員からも覚書・誓約書等を取得し，秘密保持義務や競業避止義務を明確化することが望ましい。

6. 3　他社の営業秘密の管理

アンケートにおいて，他社から営業秘密を開示された場合には，「その都度契約で取り決めた方法に従う」とした会社が53.8％であるという結果が出た。他社の営業秘密を受け入れる際には，その都度契約で取り決めた方法に従うという会社が大半なのだが，どのような点に気をつけるべきかを，以下検討する。

（1）他社の営業秘密を受け入れる際の注意点

他社の営業秘密を受け入れる場合には，当事者同士の注意を促すという意味からも，必ず，秘密保持契約を結び，自社の責任の範囲を明確にしておくことが望まれる。その上で，自社の秘密情報と区別できるよう厳格な管理が求められる。

秘密保持契約を締結した場合は，開示された情報が営業秘密に該当しない場合であっても，契約上の義務を負うこととなり，それに反した場合には，債務不履行となることは注意点としてあげられる。

（2）具体的な実務上の運用について

実際，他社の営業秘密の管理についてどのような運営がなされるべきかを検討したい。

まず自社と他社の営業秘密については特に違いを意識して管理することが望まれる。なぜならば，自社の営業秘密が漏洩した場合は，自社が損害を被るだけだが，他社の営業秘密を漏洩させた場合には，当該他社との訴訟に発展する可能性があり，マスコミ等の外部機関を通じて営業秘密が漏洩したという事実が公表されると，企業の社会的信用を失墜させかねないためである。秘密情報の提供を受ける場合には，秘密保持契約を締結し，秘密保持義務があることを改めて認識することが求められる。

では，他社の営業秘密を適正に管理するために，どのような運用をすべきか。次のような運用が考えられる。

① 他社の営業秘密は秘密保持契約に従い，秘密として取り扱い，また，流用禁止，

開示者制限などの義務にも留意して，他社の営業秘密を取り扱う役員及び従業員にその義務を周知徹底させる。

② 他社との秘密保持契約においては，相手方の営業秘密の具体的な管理方法・手続を規定されていない場合，自社の営業秘密として自社の営業秘密の管理規定に従い管理することが望ましい。

③ 秘密保持契約が無い場合の他社の開示情報管理については，あらかじめ情報管理マニュアルとして明確に定めておくと，他社情報の管理者は，管理しやすい。

④ 他社の営業秘密を当該他社の承諾を得て外部委託先に開示する場合においても，当該外部委託先から当該他社との契約おいて自己が負う義務と同等以上の秘密保持義務を課す。

(3) まとめ

他社から開示された営業秘密については，受入時に秘密保持契約を結ぶ等の理由から，営業秘密の重要性を特に意識して管理しているという会社が大半（53.8%）であると考えられる。他社の営業秘密は,漏洩等の問題が生じた場合,相手方への対応次第で訴訟へと発展する可能性もあり，自社の営業秘密以上に慎重に取り扱うことが肝要である。

6. 4　他社の営業秘密の返還

他社との秘密保持契約，共同研究開発契約において秘密情報の返還義務が定められている場合において，秘密情報の返還に関しては実務上次のような論点があると考える。

① 契約に定められた返還義務に基づき，実際に返還作業は行われているか？

② 秘密情報が返還されないで残っていると守秘義務期間中であれば契約に違反して情報が漏洩し，また，守秘義務期間後にあってはこれを流用されるリスクがある。

③ 有体の秘密情報を全て返還しても，受領者に記憶された秘密情報までは削除されるわけではない。それでもって漏洩や流用は生じないと考えられるのであろうか。反って，受領者が記憶が曖昧になることにより，意図せずして漏洩や流用をしてしまうおそれはないであろうか。

④ すべて返還してしまうと，後日受領者は開示者からどんな情報を受け取ったのか確認できないのではないか。

このうち，③に関連して，秘密情報をすべて返還しても人間の頭脳に記憶されている秘密情報までは消すことはできない上に，実際には受領者の作成した二次資料に秘密情報を含むからといって,返却を要求することには無理がある。とする考え方がある。また，秘密情報をすべて返してしまうと相手方から何を開示されたのかがわからなくなってしまい，反って意図せずして秘密情報を漏洩したり使用したりしてしまうおそれがあるとする考え方もある。このような考え方のもと欧米の契約では,「秘密情報の確認のためのコピー一式を除きすべて秘密情報を返却する」という取決めをすることもあるようである。

守秘義務に関する契約を締結する際は，返却・廃棄義務の違反とならないよう秘密情報の管理･返却に関して十分議論のうえ取り決める必要がある。

秘密情報は，一旦開示してしまうと相手方の記憶に残り，また二次資料も作成される。すなわち，どうしても回収不可能なものが生じる。また，契約において有限の守秘義務期間を定める限りは,それ以降は公知情報となってしまう。すなわち，ある期間が経過後は所有者の管理を離れ，開示先がその秘密情報を自由に使用・開示できるようになることも考えなくてはならない。よって守秘義務期間が有限の場合には特に，

開示した秘密情報を回収を考える以前に，相手先の情報管理体制の信頼性，情報のコンタミ等，相手先への開示の是非を社内で検討したうえで開示すべきであると考える。

7．おわりに

一言で営業秘密の管理といっても，様々な不法が考えられ，法的保護を目指すのか，漏洩，侵害等からの保護を最優先するのか，利用する場合の効率性を重視するのかといった会社方針によっても管理方法は大きく異なる。オールマイティな解決方法とまでは言えないが，各社，管理方法を検討する際の一参考情報にして頂ければ幸いである。

注　記

1） 不正競争防止法第２条第６項に定義されている「営業秘密」の３要件「秘密管理性」「有用性」「非公知性」のうちの一つで，アクセス制限や秘密である旨の表示等により，客観的に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をいう。
2） 東京地判H12.9.28［H8(ワ)15112］
3） 大阪地判H11.9.14［H10(ワ)1403］
4） 大阪地判H19.5.24［H17(ワ)2682］，大阪地判H17.5.24［H15(ワ)7411］，大阪地判H12.7.25［H11(ワ)933］
5） 東京地判H12.10.31［H10(ワ)4447, 13585］
6） 名古屋地判H20.3.13［H17(ワ)3846］，大阪高判H14.10.11［H12(ネ)2913］
7） 大阪地判H20.6.12［H18(ワ)5172］
8） 独立行政法人情報処理推進機構が2008年10月２日に公表した情報（URL：http://www.ipa.go.jp/security/txt/2008/10outline.html）によると，パスワード解析ツールを用いれば，大文字小文字の区別がない英字の場合，４桁であれば約３秒で解読される。またこの様な懸念から，ネット取引での個人認証などは，開設者により文字，数字，記号を併用した６桁から十数桁のパスワード設定を求めており，取引時毎にパスワードが変更されるものなどもある。
9） ①東京地判H12.10.31［H10(ワ)4447, 13585］
②大阪高判H14.10.11［H12(ネ)2913］
③東京地判H14.12.26［H12(ワ)22457］
④名古屋地判H20.3.13［H17(ワ)3846］
⑤大阪地判H19.5.24［H17(ワ)2682］
10） 米Verdasys社の「DigitalGuardian」など
11） 福岡地判H14.12.24［H11年(ワ)1102, 3694, 3678］
12） 名古屋地判H20.3.13［H17(ワ)3846］
13） 大阪地判H19.5.24［H17(ワ)2682］
14） 東京地判中間H14.12.26［H12(ワ)22457］
15） 東京地判H17.6.27［H16(ワ)24950］
16） 田村善之・津幡笑「商標・意匠・不正競争判例百選」別冊ジュリストNo.188　95　有斐閣
17） 東京地判H11.7.23)（判時1694号138項）
18） 東京地判H18.7.25［H16(ワ)25672］
19） 大阪地判H10.12.22［H5(ワ)8314］
20） 東京地判H14.8.30［H13(ワ)21277］

（原稿受領日　2009年３月17日）