営業秘密に関する情報セキュリティ管理
改正不正競争防止法など相次ぐ立法措置と企業の課題

岡野靖丈

CONTENTS

要約

1　1990年代以降、技術、ノウハウといった営業秘密が東アジア諸国の企業などに不用意に流出する事態が相次いだ。一方、終身雇用制の崩壊から労働者の流動性が高まるとともに、契約社員や派遣社員も職場に急増するなど、営業秘密を取り巻く社会的環境が大きく変わっており、その漏洩の危機が高まっている。

2　2005年４月に個人情報保護法、同年11月に改正不正競争防止法がそれぞれ施行された。今後、2006年５月に新会社法、2009年に日本版SOX法（金融商品取引法）が施行される予定であり、相次ぐ法改正と新法施行によって、企業は一層厳格な情報セキュリティ管理が求められる。

3　特に改正不正競争防止法の施行により、国内の営業秘密が海外で漏洩された場合も訴訟の対象になるとともに、従業員だけでなく法人の処罰も可能になった。また、損害賠償と刑事罰が強化され、法的な対応が進んでいる。

4　このような変化に対する企業の対策としては、自社のどの部門、どの業務にどのような情報が存在し、いかに管理されているかを精査することが出発点になる。また、自社の強みがどこにあり、どの部分がどのような営業秘密に立脚したものであるかを明確に認識し、そのうえで組織的、システム的、物理的に、それらを適切に管理することが重要である。そのためには、組織対応、人事対応、システム対応、企業・社員間の秘密保持契約や教育研修内容の見直しなどの改革が必要になる。

Ⅰ　多発する技術、ノウハウなど営業秘密の漏洩

1990年代以降、技術、ノウハウなどの営業秘密（企業にとって有用で、かつ非公知で秘密に管理されている情報）が東アジア諸国の企業などに不用意に流出する事態が問題視されてきた。たとえば、日本メーカーの優秀な技術者が海外の競合企業から数倍の年俸で引き抜かれ、重要な生産技術が移転した。従業員が週末に海外に出向いて、競合企業に技術指導するといったケースも見られた。このため、日本政府や企業は警戒感を強めてきた。

一方、国内では、企業と従業員の関係が大きく変化している。終身雇用制の崩壊から労働者の流動性が高まるとともに、契約社員や派遣社員が職場に急増している。実際、これまで営業秘密漏洩に関する民事訴訟の半数以上に退職者が関与しており、さらに契約社員や派遣社員がかかわる事件も増えている。

また、ここ数年、顧客リストの売買、牛肉産地の偽装、自動車のリコール隠し、銀行員の使い込みなど、高いロイヤルティ（忠誠心）のもとで性善説を基本とした日本の企業経営の根幹を揺るがす事件が多発している。

さらに、アウトソーシングが業務効率やコスト削減のために進められてきた。情報通信技術の進展のもと、重要な営業秘密がネットワーク上で送受信される機会も増えている。2000年２月に不正アクセス禁止法が施行され処罰対象となったにもかかわらず、不正アクセスの届け出件数は2004年に5000件を突破し急増している。こうした社会的要因が複合的に作用し、企業の営業秘密が国内外問わず、漏洩しやすい環境をつくり出している。

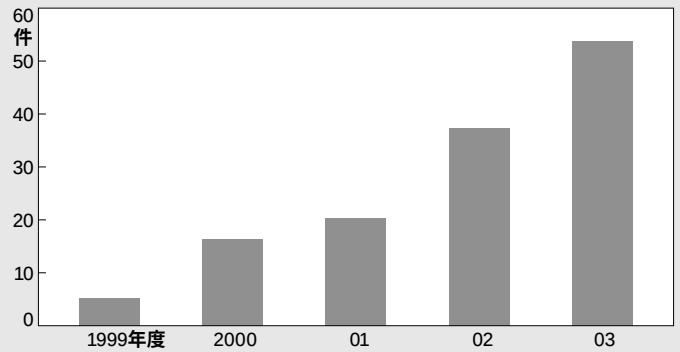
Ⅱ　相次ぐ法改正、新法施行による規制強化

多発する個人情報漏洩事件に対応するため、2005年４月には個人情報保護法が施行された。個人データ（個人情報を容易に検索できるように体系的にまとめたデータ）の安全管理措置の要求水準が高くなり、企業はハード、ソフト両面で対応を迫られている。

また、企業の知的財産などを保護する法規定が強化され（知的財産基本法２条１項）、改正不正競争防止法も2005年11月に施行された。後者では、両罰規定（従業員などが処罰された場合、事業主〈法人を含む〉をも処罰する規定）により、法人処罰が強化された。ここ数年、不正競争防止法関連の訴訟が急増しており、企業の情報セキュリティ管理に対する意識も変化している（図１）。

一方、アメリカのSOX法（サーベンス・オクスリー法：企業改革法）404条が、外国企業登録の日本企業にも、2006年７月15日以降に終了する事業年度から適用され、SEC（証券取引委員会）へ提出する書類に「虚偽や記載漏れがないこと」「内部統制の有効性評価の開示」などを保証する証明書と署名を添付することが要求されている。不正があっ

図1　増加する不正競争防止法違反の起訴件数



出所）経済産業省の資料より作成

た場合、CEO（最高経営責任者）には罰金または禁固刑の刑事罰が設けられている。

2009年には、内部統制法といわれる日本版SOX法（金融商品取引法）が日本でも施行される予定であり、さらに、2006年５月に施行される新会社法は、資本金５億円以上または負債200億円以上の企業の経営層に対し、内部統制の整備について決定、管理することを義務づけている。

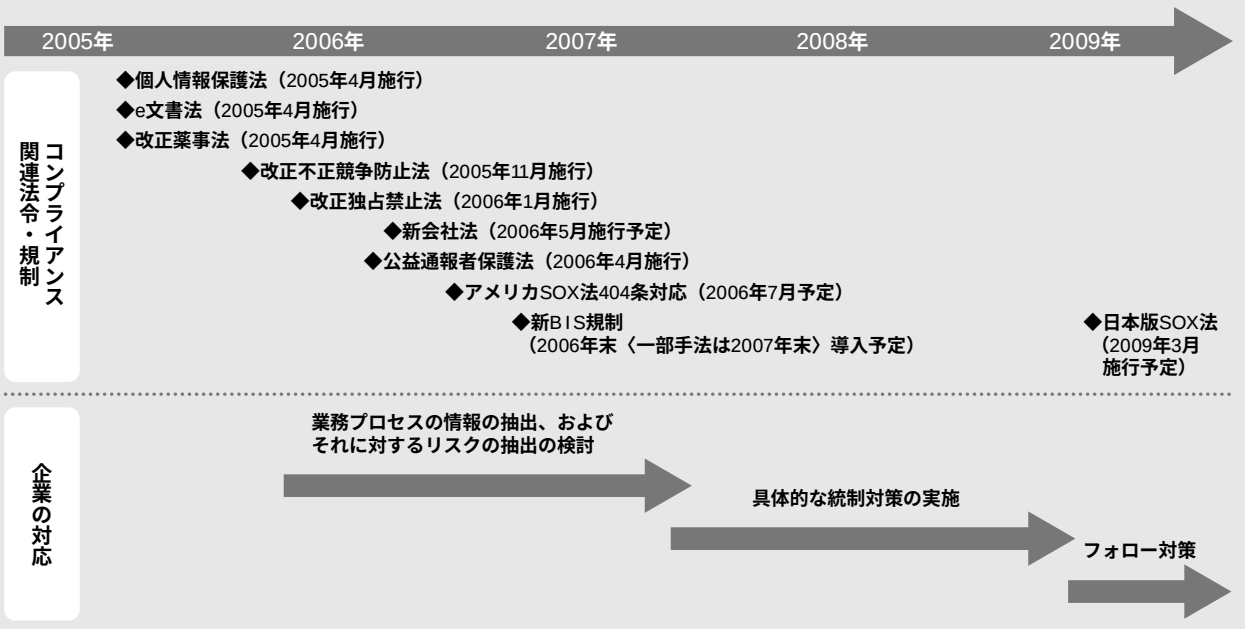
今後、企業が営業秘密漏洩などの企業リスクをいかに管理するかは、社内の業務プロセスをどう統制するかという観点で見る必要がある。現在、企業の情報セキュリティ管理のあり方は重要な経営戦略になっているが、営業秘密漏洩も、自社の知的財産の流出だけでなく、取引先、消費者、株主などとの信用問題に関係し、ひいては株価に直接影響し、経営層の処遇にも進展する重大な問題である。

このほか、2006年末、BIS（国際決済銀行）は銀行の信用リスク、市場リスクに加え、情報漏洩を伴うオペレーショナルリスク（事務、システム運営など日常業務にかかわるリスク）も加味した自己資本比率規制（新BIS規制）を適用する予定であり、金融業界にもより強固な内部統制が求められる。

他方で、企業の情報操作などの不正を摘発しやすくする改正独占禁止法が2006年１月に施行されており、公益通報者保護法も４月に施行された。改正独占禁止法の主要なポイントは、司法取引であるリーニエンシー制度の導入と、課徴金の引き上げにある。これにより多様な情報操作、情報漏洩、談合・カルテルなどが暴きやすくなる。

このように、個人情報保護法、改正不正競争防止法、日本版SOX法など、情報漏洩を含む企業の不正に対する法規制が相次いで強化されており、経営層にはあらゆる不正を許さない内部統制の具体的な施策が求められている。すでに多くの企業がこの対応に迫られており、多額の投資を余儀なくされている。

図2　コンプライアンス関連法令・規制と想定される企業の内部統制対応ロードマップ



注）BIS：国際決済銀行、e文書法：「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」と関係法の総称、SOX法：サーベンス・オクスリー法（企業改革法）

III　改正不正競争防止法の施行と営業秘密管理

1　個人情報保護法との比較

営業秘密としては、技術、ノウハウ、顧客情報といった企業情報が中心となるが、前述したもののうちでも、不正競争防止法が最も関係する法規制である。個人情報保護法は顧客情報を中心とした個人情報が関係するが、あくまでも民事での扱いになる（表１）。

営業秘密を保護するには、不正競争防止法をよく理解し、有効に活用する必要がある。同時に、自社の従業員が他社の営業秘密を侵害しないための防止策、万一侵害したときの対処策を講じるためにも、同法を把握しておくことが必要となる。

個人情報保護法は、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しており（１条）、個人情報とは、生存する個人に関する情報であって、氏名、生年月日、住所など個人を識別することができるものである（２条１項）。

同法は、5000件以上の個人情報を保有し、事業に利用している「個人情報取扱事業者」に対して個人情報の適正な取り扱いを求める法律であり、同事業者が規制の対象となる（２条３項）。個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的をできる限り特定しなければならず（15条）、また、あらかじめ本人の同意を得ないで、15条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない（16条）。

さらに個人情報取扱事業者は、個人データの取り扱いの全部または一部を委託する場合は、その個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わねばならない（22条）。また、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない（23条）。

一方、不正競争防止法は不正競争の１つとして、「営業秘密を保有する事業者からその営業秘密を示された場合において、不正の競業その他の不正の利益を得る目的で、又はその保有者に損害を与える目的で、営業秘密を使用し、又は開示する行為」（２条１項７号）を規定している。

営業秘密は、秘密管理性、有用性、非公知性を要件とするが（２条４項）、秘密管理性は、営業秘密へのアクセス制限と、その情報が秘密に管理されているという客観的認識が必要となる。裁判上これが営業秘密に関する最も重要な争点となっている。有用性については、客観的にそれが経営上重要な情報であることを証明しなければならない。非公知性では、社員全員が知っているものや、刊行物などにすでに掲載されているものは該当しな

表1　不正競争防止法と個人情報保護法の比較

	不正競争防止法	個人情報保護法
保護対象情報	●営業秘密（知的財産、ノウハウ、顧客名簿など）	●氏名、生年月日、住所など個人が識別可能な個人情報
保護対象者	●営業秘密保有企業	●生存する個人
規制対象者	●従業員、退職者、企業など	●個人情報取扱事業者
主な規制対象行為	●営業秘密の不正取得・使用・開示	●個人情報利用目的以外の使用 ●不正取得 ●情報の正確性★ ●第三者への情報提供 ●安全管理措置★
罰則など	●差し止め請求、損害賠償 ●5年以下の懲役または500万円以下の罰金、両罰規程	●主務大臣からの勧告・命令 ●上記に違反した場合、6カ月以下の懲役または30万円以下の罰金

注）★印は、個人情報取扱事業者にその確保が義務づけられる
出所）那須野大『不正競争防止法による知的防衛戦略』日本経済新聞社、2005年より作成

い。代表的には、マル秘文書や極秘押印資料のようなものが、これに該当する。

これに対するアクセス規制としては、「窃取、詐欺、強迫その他の不正の手段により営業秘密を取得する行為又は不正取得行為により取得した営業秘密を使用し、若しくは開示する行為」（２条１項７号）が禁止された。

個人情報保護法は、個人情報取扱事業者が規制対象であり、内部犯行による情報漏洩だったとしても、企業が勧告、命令などの行政措置などを受ける。しかし、不正競争防止法により、漏洩した顧客情報群が営業秘密として認定されれば、不正競争のために取得、使用した社員や企業が民事罰、刑事罰の対象となる。被害者として、営業秘密漏洩に関する訴訟を起こす場合は、不正競争防止法を適用するケースが多くなる。

2　日本国外における営業秘密の不正使用・開示に対する防衛策

改正前の不正競争防止法では、営業秘密が日本国外で不正使用・開示された場合には、処罰の対象外だった。改正不正競争防止法では、日本国内で管理されていた営業秘密を、詐欺等行為や管理侵害行為により取得し（21条４項）、日本国外で不正使用・開示した者にも適用される。また、海外で営業秘密を不正の手段により取得し、それを日本国内に持ち込んで使用または開示する行為も処罰の対象になる。しかし、海外子会社で情報を不正取得されて、海外で使用された場合には、不正競争防止法の侵害には当たらない。

この法律は、抑止力にはなるが、あくまでも事後的救済措置である。海外の競合他社に営業秘密が使用・開示された場合には、従来多くの日本メーカーが経験したように、当該企業が取り返しのつかない損害を被ることになる。企業としては、将来キーとなる技術を利用した開発、生産はできる限り国内で行うような施策や、海外生産拠点での作業のブラックボックス化など、より積極的な防衛策を講じておくことが必要である。

3　退職者による営業秘密の不正使用・開示について

改正前の不正競争防止法でも、退職者が媒体に記録された営業秘密を不正に使用・開示した場合には処罰の対象とされていた。そして、退職者が頭の中に入れて持ち出し、不正に使用・開示した場合などには、民事上の契約不履行扱いとされていた。

改正によって、「営業秘密を保有者から示されたその役員又は従業者であった者であって、不正の競争の目的で、その在職中に、その営業秘密の管理に係る任務に背いてその営業秘密の開示の申込みをし、又はその営業秘密の使用若しくは開示について請託を受けて、その営業秘密をその職を退いた後に使用し、又は開示した」（21条１項８号）場合は処罰の対象とすることに変えられた。罰則も、５年以下の懲役または500万円以下の罰金、またはこれを併科するという刑事罰が導入された。もっとも、アメリカの経済スパイ法では以前から刑事罰が導入されており、韓国などでも同様な法規制が敷かれている。

とはいえ、退職者に関しては、職業選択の自由（憲法22条１項）、職業選択の自由が構成する公序（民法90条）などを考慮する必要があり、また競業避止義務に対する近年の訴訟判決を考えると慎重な対応も必要となる。

4　両罰規定の適用

改正不正競争防止法では、役員または従業員が営業秘密の侵害を行った場合、裁判所の秘密保持命令に対する違反者がいる場合（22条１項９号）には、その行為者を根拠に両罰規定の適用を受けることになる。

法人処罰については、判例上、原則として、企業の選任監督に関する過失が推定される場合に適用されるとされているため、企業側が法人処罰を免れるには、適切な選任監督義務を果たしていたことを立証する必要がある。それが証明されなければ、22条１項により（６～８号は除外）、法人に対して１億5000万円以下、個人事業主に対しては500万円以下の両罰規定が適用される。加えて、民事的、社会的責任を問われる可能性も高く、単純に両罰規定による刑事的制裁を回避するためだけでなく、ビジネス上生じるリスクをいかに回避するかという観点で、営業秘密の侵害防止に取り組むことが求められる。

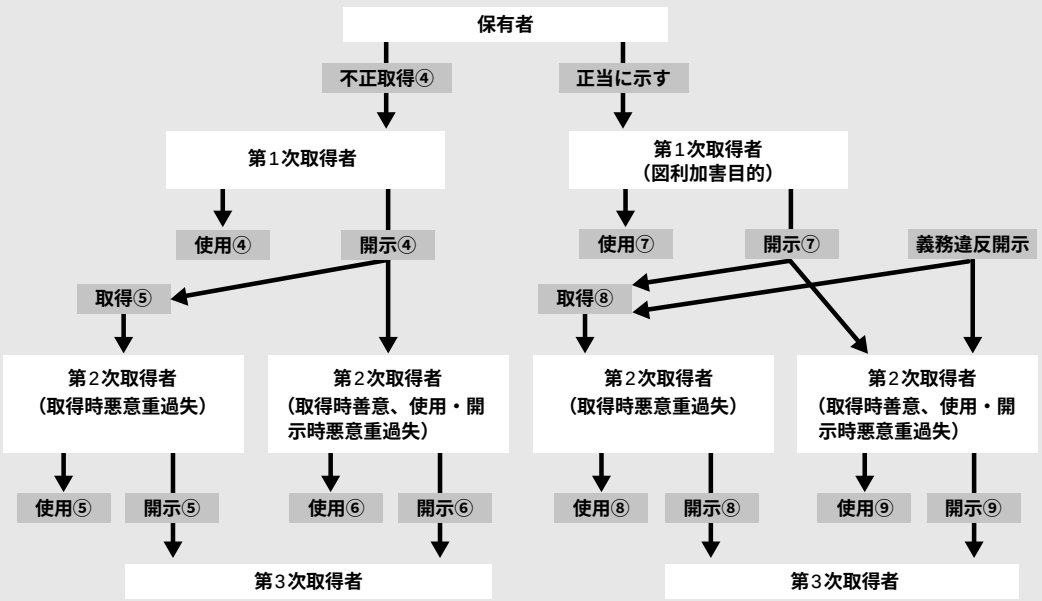
5　営業秘密にかかわる不正競争行為の各類型

不正競争防止法２条１項４～９号では、営業秘密の不正取得・使用・開示行為につき、６つの類型に分けて想定している（図３）。

まず、４～６号は営業秘密を不正取得し、またはそれにより取得した営業秘密を使用・開示するケースであり、７～９号は正当に示された後に不正使用・開示するケースである。また、４・７号は、一次的に営業秘密を不正取得または不正使用・開示する者（第一次取得者）の行為であり、５・８号は二次的に悪意過失で営業秘密を取得して使用・開示する者（第二次取得者）の行為である。

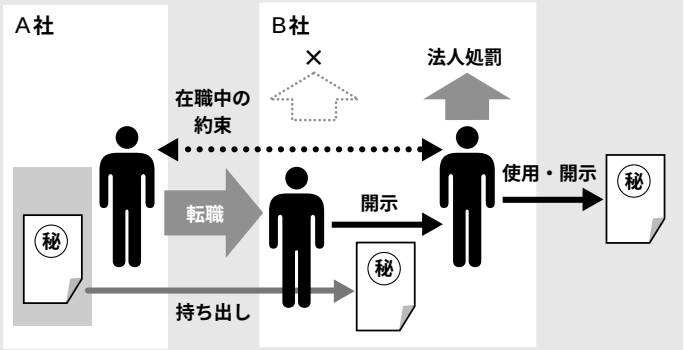
具体的には、不正取得（図の④）は、従業員が勤務先の営業秘密である受注報告書類を窃取して産業スパイに売り渡したケース（大日本印刷産業スパイ事件、東京地裁判決、1965年６月26日）や、デパート勤務の技術者が勤務先の顧客名簿が入力された磁気テープ

図３　営業秘密にかかわる不正競争行為の概要



注）④～⑨の数字は、不正競争防止法2条1項の中の、4～9号の行為類型であることを表す
出所）経済産業省

図4　営業秘密にかかわる不正競争行為の例



出所）経済産業省

を盗み、リスト販売会社に売り渡したケース（京王百貨店顧客名簿事件、東京地裁判決、1987年９月30日）などが相当する。

不正取得後の転得（同⑤）は、従業員が営業秘密を盗み、第三者が受け取るようなケースがこれに該当する。

不正取得に関する事後的悪意による使用・開示（同⑥）は、営業秘密を入手（その時点では善意）後、競業企業が介在していたことを知りながら、営業秘密を使用・開示するようなケースがこれに該当する。ただし、取引などにより入手した情報を無過失で開示した場合、適用除外規定（12条１項６号）により無罪となる。

不正取得・開示（同⑦）は、通販会社を退職した取締役が、在職中に企業を立ち上げ、前職場の従業員仲間から顧客名簿を受け取り、その名簿を通販事業に使用する行為（コルム貿易事件、大阪高裁判決、1983年３月３日）などが該当する。

不正開示後の転得（同⑧）は、製造会社A社の従業員が、在職中に同業種B社の立ち上げに参加し、A社退職時にA社と秘密保持契約を結んでいるにもかかわらず、許可なく設計図などを開示したケースなどがこれに該当する。この場合、B社も契約を知りながら、それを開示させた責任が問われる。

不正開示に関する事後的悪意による使用・開示（同⑨）は、ａ氏が営業秘密を取得後、それが不正に開示されたものと知りながら、開示するようなケースがこれに該当する。

より理解を深めるために、競合他社への転職の事例を取り上げる（図４）。

たとえば、国内の自動車メーカーA社のデザイナーだったａ氏は、１年前に転職した競合他社の外資系B社で、A社が営業秘密として管理していた、しかもａ氏の開発グループで開発していた新規デザインを、不用意にもB社の同僚ｂ氏に開示し、ｂ氏はB社の新規車種開発にそれを応用した。その新製品の外観は、かつてのａ氏の開発グループで進めていたコンセプトに非常に似ていた。従来、B社の車は市場でさほど競争力がなかったが、その斬新なデザイン性が消費者に受け、その年のグッドデザイン賞を受けた。

あまりにも自社の新コンセプトに似ているB社の新機種にA社が疑いを持ち、調べたところ、ａ氏がB社に転職していることがわかった。その年のA社の同車種の売り上げは、前年の７割まで落ち込んでいた。

この場合、A社のとるべき措置として（営業秘密が十分管理されていた場合）、ａ氏には秘密保持契約不履行につき、契約内容に沿って損害賠償を請求できる。B社に対しては当該車種の生産の差し止め請求を行える。不正開示された営業秘密を悪意をもって使用したｂ氏にも、損害賠償を請求できる。またB社には、選任監督義務不履行を理由に、両罰規定で法人処罰が適用される可能性がある。

Ⅳ　営業秘密保護に対する施策の構築

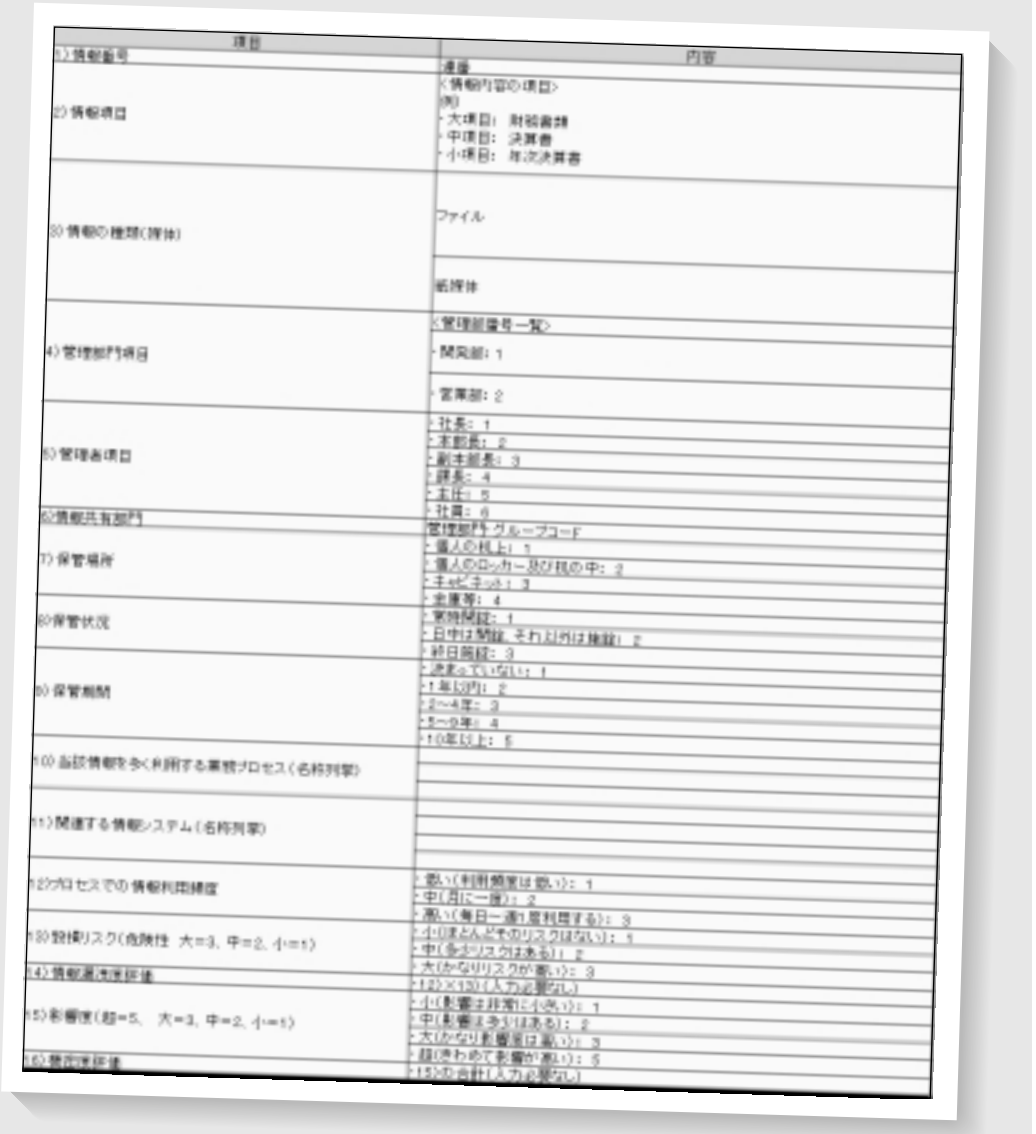
1　システム対応を中心として

（1）管理すべき情報の洗い出しとルール化

まず、そもそも企業の各業務プロセスにどのような重要情報が存在し、それが漏洩することでどんなリスクが生じるかなどの分析作業が必要になる（図５にそのための管理シートの例を示す）。つまり、全社的に情報の洗い出しを行い、その範囲・内容、機密度、リスクなどを明確にする必要がある。

自社の強みがどこにあり、どの部分がどのような営業秘密に立脚したものであるかを明確に認識したうえで、それらを組織的、システム的、物理的にそれぞれ実効的に管理することが重要である。多くの企業にとって、競争力の根幹となる営業秘密がそれほど大量にあるわけではない。また、そうした営業秘密に直接触れる者は限定されているはずであ

図５　情報資産管理シートの例



項目	内容
(1) 情報番号	連番
(2) 情報項目	<情報内容の項目> 例) ・大項目：財務書類 ・中項目：決算書 ・小項目：年次決算書
(3) 情報の種類(媒体)	ファイル 紙媒体
(4) 管理部門項目	<管理部署番号一覧> ・開発部：1 ・営業部：2
(5) 管理者項目	・社長：1 ・本部長：2 ・副本部長：3 ・課長：4 ・主任：5 ・社員：6
(6) 情報共有部門	管理部門グループコード
(7) 保管場所	・個人の机上：1 ・個人のロッカー及び机の中：2 ・キャビネット：3 ・金庫等：4
(8) 保管状況	・常時開錠：1 ・日中は開錠、それ以外は施錠：2 ・終日施錠：3
(9) 保管期間	・決まっていない：1 ・1年以内：2 ・2～4年：3 ・5～9年：4 ・10年以上：5
(10) 当該情報を含む/利用する業務プロセス(名称列挙)	
(11) 関連する情報システム(名称列挙)	
(12) プロセスでの情報利用頻度	・低い(利用頻度は低い)：1 ・中(月に一度)：2 ・高い(毎日一週1度利用する)：3
(13) 登録リスク(危険性 大=3、中=2、小=1)	・小(ほとんどそのリスクはない)：1 ・中(多少リスクはある)：2 ・大(かなりリスクが高い)：3
(14) 情報漏洩度評価	(12)×(13)(入力必要なし)
(15) 影響度(超=5、大=3、中=2、小=1)	・小(影響は非常に小さい)：1 ・中(影響は多少はある)：2 ・大(かなり影響度は高い)：3 ・超(きわめて影響が高い)：5
(16) 機密度評価	(10)の合計(入力必要なし)

る。何もかも営業秘密になってしまえば、そのような大量の営業秘密を厳格に管理することはほぼ不可能だろう。

また、そのような情報をいかに処理するかといったルールが必要になる。たとえば、以下のものは最低限整備すべきである。

- 情報取得の適正化（情報の出所の明示、侵入や不正な利益の提供など不正な手段での情報入手の禁止、部の責任者などによる情報の入手経路の明確化、等）
- 情報管理の適正化（他社情報を預かった場合の社内手続き、他社情報の管理方法、他社情報と自社情報の明確な分離と混合の防止、他社営業秘密に関する中途採用者の責任、等）
- 侵害に対するコンティンジェンシープラン（侵害が発覚した場合の調査や情報伝達に関する社内手続き、侵害を行った従業員に対する懲戒・刑事告発などを行うための社内手続き、他社情報が流出した場合の被害者に対する損害回復措置、他社情報が流出した場合の関係者の懲戒処分、問題事実の公開、重要事項の迅速・的確な取締役会への報告体制の整備、社内通報制度、等）

一方、自社の有する技術・ノウハウ領域の重要性や、メーカー・材料系企業であれば、技術ごとの競争力、国別の知的財産保護の状況（法制度の整備、権利の侵害、取り締まり等の運用）、海外への技術移転に関するリスクなどの分析が同時に必要となってくる。

（2）物理的、システム的対応

不正競争防止法に関する訴訟で主な争点と

表2　営業秘密の秘密管理性を争点とした判例（抜粋）

判例	情報種別	秘密管理性	争点
2000年 9月28日 東京地裁	●治験データおよび輸入申込書などの紙媒体 ●顧客名簿	×	●施錠する鍵が付いていたが、勤務時間中は施錠されていなかった ●一部の書類に「マル秘」など秘密として管理されていることを示す表示を付すような取り扱いはされていなかった
2000年12月 7日 東京地裁	●顧客に関する契約内容一覧表および車両変動状況表 ●管理車両および運転者一覧表	×	●当該情報については、原告会社の従業員ならアクセスできる状況にあった ●アクセス制御のパスワードや、営業秘密であることを示す標識が付されていなかった
2001年 9月26日 大阪地裁	●顧客情報	×	●厳重に管理されていたことを裏付ける証拠がなく、原告が資料ノートを自宅に持ち帰って営業活動を行うことを許していた ●従業員に対し営業秘密の保持について訓示していた証拠がなく、従業員の退職に際し、顧客情報の開示・利用を禁じる誓約書を徴収していなかった
2002年 7月18日 大阪地裁	●顧客名、継続的取引のなかで培われた個々の顧客の商品に対する要望など	×	●顧客名簿による管理すら行っていなかった ●顧客情報についても、原告から特段の情報管理を要請されていたわけではなく、これを利用したカタログを作成して広く頒布した
1998年12月22日 大阪地裁	●ノズルの技術	○	●従業員から誓約書を徴して営業秘密の保持を義務づけた ●在庫管理を製造課長が行い、製造課の部室のロッカーに保管し、技術を管理していた ●部外者は、市販品を加工していること自体は理解できても、具体的にどの部分をどのように加工したかを知ることは困難であった
2003年 2月27日 大阪地裁	●設計電子データ	○	●本件電子データは、メインコンピュータのサーバーにおいて集中保存され、アクセス者が限られていた ●設計業務には、社内だけで接続されたコンピュータが使用され、設計業務に必要な範囲内でのみデータにアクセス可能で、バックアップ作業は特定の責任者だけに許可されており、従業員全員が本件データ取り扱いの様態を理解していた

出所）牧野利秋監修、飯村敏明編集『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、2005年より作成

なっているのは秘密管理性である（表２）。この点を立証できなければ、訴えを起こしても敗ける可能性が高い。たとえば従業員全員がアクセスできるようなものは、秘密に管理しているとはいえない。情報の洗い出しの時点で、その営業秘密にアクセスできる人物を限定する必要がある。

システム的には、サーバールームには生体認証、IC（集積回路）カードなどの認証システムとカメラを設置し、外部から持ち込んだパソコンがネットワークに接続された場合、警報が鳴るなどの処置も考えられる。また、ウェブ、メールや、HDD（ハードディスクドライブ）内データの消去・編集などの追跡と管理は非常に重要である。

実際、ログ（記録）の改ざん、破壊、不正アクセスの追跡などを行うために、ツールを利用してデジタル的に証拠を押さえ、刑事訴訟、民事訴訟などの法的問題の解決を図るコンピュータフォレンジックスという手法が、アメリカを中心にすでに認知されている。信頼を得られる手段で、証拠を集め、分析を行うことはリスク管理上必須となる。

紙文書からの漏洩も重要な問題である。実際、日本ネットワークセキュリティ協会によれば、2004年度の内部犯行による情報漏洩の46%が紙文書経由という。重要書類の持ち出しには管理シートなどでのチェックが必要だが、複製物に対してもICカードなどによる個人認証やプリント制限など、内部者による漏洩抑止策を促進すべきである。一方で、秘密管理の実質を形式的に立証するには、「極秘」「マル秘」などの具体的な表示も必要である。過去の判例では、この表示がないことで敗訴しているケースがある。

盗難のような事故も想定すべきである。企業のパソコン、携帯端末などについて、パスワード等による認証管理や、セキュリティソフトを使用するなどの対応は当然だが、そもそも重要な顧客情報をノートパソコンに入れて持ち歩くようなことは避けるべきである。それが難しいならば、HDDを搭載しないディスクレスパソコンの検討も考えられる。

2003年のアメリカ経営協会とｅポリシー・インスティチュートの共同調査によれば、アメリカでは、ネットの悪用を理由に従業員を解雇した経験のある企業が26%に達し、25%が電子メールの悪用、６%が電話の悪用を理由に解雇している。55%の企業が電子メールを保管・検閲している。20%の企業が裁判所や監督機関から電子メールの提出を求められた経験を持ち、従業員の電子メールが原因の訴訟問題を抱える企業も13%に上る。

電子メールやインターネットの利用状況が、裁判などで証拠として扱われるケースが増えているため、コンピュータフォレンジックス的アプローチはますます必要となる。

2　組織対応を中心として

（1）取締役、監査役などの機能強化

企業グループ全体の情報管理における内部統制を進めるに当たって、取締役、監査役の管理機能が非常に重要であることはいうまでもない。代表取締役、当該業務を担当する取締役は、これらの事項に関する取締役会の決議を受け、具体的な体制の整備を行うことが求められるとともに、法令遵守と業務適正のための体制整備に関する取締役会の決議の概要を事業報告に記載しなければならない（株式会社の業務の適正を確保する体制に関する

法務省令案７条)。

また、監査役・監査役会（監査委員会）は、取締役会の決議に基づいて代表取締役などがこのような体制を有効に整備しているかなどの点について監査し、取締役会の決議が相当でないと認められるときはその旨およびその理由を記載した監査報告を作成しなければならない（８条)。

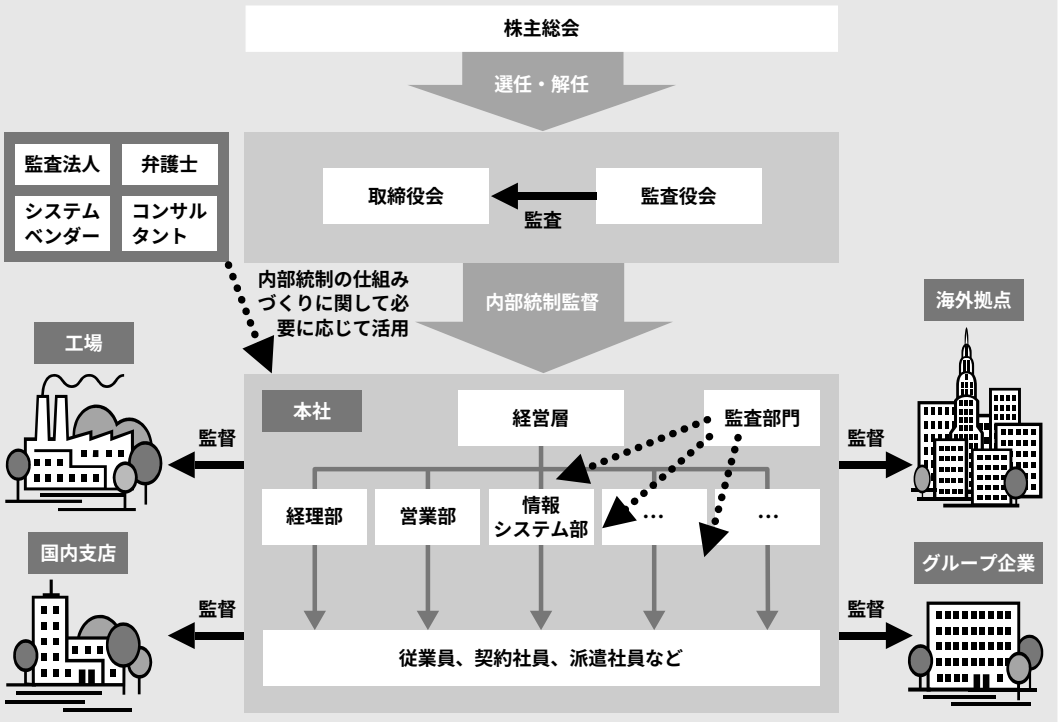
取締役会は、法令遵守とリスク管理のための基本方針を決定する必要がある。まず、法令遵守やリスク管理をめぐる企業不祥事の多くに取締役などの関与が見受けられるため、法令遵守と適切なリスク管理体制の整備の前提として、コーポレートガバナンス（企業統治）の確立が必要である。一方、代表取締役などは、法令遵守、リスク管理を確保するための体制を整備する責任を有する。体制の構築、運用に際しては、トップが法令遵守、リスク管理の重要性を全社員に認識させるような取り組みを行う必要がある。

取締役会、代表取締役などによる内部統制システムの整備状況は監査の重要事項となる。監査役・監査役会は、取締役会の法令遵守とリスク管理のための体制整備の基本方針に関する決議が適正かつ妥当であるか、また代表取締役などが取締役会の決議に従って、法令遵守、リスク管理の体制を構築しているか、有効に運用されているかなどについて監査しなければならない（図６)。

法務省令案では、監査役の監査の実効性を確保するためのさまざまな体制は、業務の適正を確保するための体制に含まれるとしている（５条３項など)。それは本社だけでなく、グループ企業、関連企業を含めて対応することが必要になる（５条１項５号など)。

また、2006年５月施行予定の新会社法では、内部統制の整備について決定することが企業に義務づけられ、取締役や監査役は法令

図６　取締役会、監査役会と内部統制



遵守、リスク管理のための体制の整備・運用の責任を負っている（348条３項４号、同条４項、362条４項６号、同条５項、416条１項１号、同条２項）。大和銀行株主代表訴訟の判決（大阪高裁、1997年12月８日）でも、取締役は法令を遵守するだけでなく、従業員が職務を遂行する際、違法な行為に及ぶことを未然に防止するための法令遵守体制を確立すべき義務があるとしている。

経営層、従業員の情報漏洩不正を管理するためには、取締役、監査役を中心とした客観的で有効な管理が必要になってくる。

（２）秘密保持誓約書の運用

機密情報管理規定、倫理管理規定など自社の管理規定を整備し、従業員に徹底する必要があるが、それを前提として、従業員との秘密保持契約を整備すべきである。

①秘密の範囲の具体的規定

営業秘密などの重要情報の管理を徹底するうえで、従業員が秘密保持誓約書を提出するよう促進する必要がある。既出の過去の判例でも秘密管理性（不正競争防止法２条４項）が裁判上の争点になっているケースが多く、企業が秘密に管理していたと証明する意味でも、誓約書の有無は裁判上、非常に大きな意味を持つ（岩城硝子ほか事件、大阪地裁判決、1998年12月22日）。

東京リーガルマインド事件の判決（東京地裁、1995年10月16日）では、個別に従業員から誓約書を取り付けなくても、就業規則で、退職後も含めた秘密保持条項を定めておけば、同条項により、退職後も秘密保持義務を法的に強制することは可能と考えられている。しかし、就業規則の秘密保持条項について、総合職採用の場合、一般的に「職務上知り得た営業秘密」のような包括的な内容にならざるを得ず、退職後に関しては法的拘束力が否定される可能性も十分ある。また、退職時に従業員に強制することは難しい。

したがって、入社時の秘密保持誓約書で、「秘密の範囲を限定した誓約書の追加提出が求められた場合には、これに応じなければならない」などの旨を約定することが重要となる。メーカーなどの技術者採用の場合、入社時から秘密の範囲を限定することは十分可能であり、誓約書を提出させるべきだろう。

また、入社時に秘密保持誓約書を提出しなかったとしても、それをもって従業員としての重大な服務規律違反または背信行為とすることは困難であるが、その企業の業務内容や当該社員の業務内容などに照らして、誓約書の提出を求める必要がある。個別のプロジェクト参加時や退職時には、入社時と異なり、「秘密の範囲」が限定されているケースが多いので、なるべく詳細な記述を条項に入れることを推奨する。

たとえば、「A薬品製造のためのB工程の調合手順」「C研究グループが2002年から2005年に研究開発してきたD技術」「ファイルEの200～250ページに記載された情報」のように、できる限り、具体的な内容を明確にすることは重要である。

次に、営業秘密が化体された媒体（書類、電子ファイルなど）や装置などを特定することで、間接的に情報を特定する方法がある。例としては、「ABCと題するマニュアル」「C株式会社がD氏に提供したA001号図面」「自社が製造、販売する商品型番にして、X－１、X－２と表示されているものと同規格のも

の」などの媒体の表記があげられる。

また、消費者向け製品・サービスを扱う企業を中心として、個人情報保護法20条の「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない」との規定を受けて、個人情報の非開示条項を秘密保持誓約書に明記することも考えられる。

契約の締結などはプロジェクト参加時が好適だが、情報の特定は終了時に確認するなどの手続きが必要だろう。その際に、特定の秘密保持義務は退職後にも存続することなどについて、了解を得ることが重要である。

②退職時の秘密保持契約

従業員が退職する場合には、在職中に締結した秘密保持契約の内容も踏まえ、最終的な情報の特定を行ったうえで秘密保持契約を締結し、または就業中に締結した契約に基づいて適切な秘密保持契約を結ぶ。

また、企業の基幹的な営業秘密を保有している従業員が退職する際は、秘密保持契約締結時に「退職後秘密を漏洩・流用しない」という条件に同意した者にのみ、秘密保持の代償部分を通常の退職金に加算するといった退職金制度の再設計も検討に値する。さらに、退職者による背信性の高い営業秘密の漏洩・流用に対処するため、就業規則に退職金の没収・減額条項を整備しておく必要がある。

常に上記のすべてのプロセスを踏む必要があるわけではないが、こうした段階を追った義務の付加と情報の収集に関して、社内的に手続きを明確にしておくことが望ましい。

③競業避止契約と職業選択の自由

競業避止契約（退職後、競合他社に就職したり、競合企業を設立したりしてはならないことを取り決める契約）は、営業秘密の保護を外形的に担保するために締結されることがある。しかし、秘密保持契約と異なり、直接的に退職者の転職を制限するものであり、秘密保持契約に比べて憲法上の職業選択の自由を制限する蓋然性が高いため、判例でも、競業避止契約の有効性は、秘密保持契約の有効性以上に厳格に解されている。

具体的には、秘密保持契約の場合、「その秘密の性質・範囲、価値、当事者（労働者）の退職前の地位に照らし、合理性が認められるときは、公序良俗に反せず無効とはいえない」とされているのに対し、競業避止契約については、「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といった諸般の事情を総合して合理的な制限の範囲にとどまっていると認められるときは、その限りで、公序良俗の観点より無効とされる場合が多い」とされている（ダイオーズサービシーズ事件、東京地裁判決、2002年８月30日）。

④包括的な秘密保持契約は無効の可能性

最近になって、従業員と秘密保持契約を結ぶケースが増えているが、保持すべき営業秘密の内容を特定していない場合が多い。たとえば、よく見られるのは「A社で知り得た営業秘密については、在職中はもとより、退職後にも一切第三者に開示・漏洩いたしません」といった内容だが、これでは法的拘束力を否定される可能性がある。また、「A社で知り得たことすべての営業秘密」といった契約は民法の公序良俗違反で無効になる可能性があり、訴訟上効果が弱いと考えられる。

企業にとって重要なのは、経営に大きな影

響を与えるような営業秘密が何であるかを認識し、物理的、システム的、組織的に適切に管理することである。また、その情報を取り扱う者を特定し、情報の取り扱い方法を規定するとともに、その情報を生み出した人を含め、コア人材の流出に伴う営業秘密の漏洩を防ぐための体制を整備することである。

特にこうした管理の問題は、大企業になればなるほど深刻である。これは、秘密保持契約の対象となる情報や従業員が膨大なため、経営全体についての理解が共有されないまま法務部や知財部、総務部などに営業秘密管理を任せてしまい、営業秘密も対象者も十分に特定できずに実効的な秘密管理もできないという事態が生じかねないからである。

（3）セキュリティに対応した組織

多発している企業の個人情報流出事件を契機に、企業内でCISO（情報セキュリティ管理の統括責任者）を導入する企業が増えている（図７）。コンピュータシステムやネットワークセキュリティ対策だけでなく、機密情報や個人情報の管理についても統括するケースが多い。各部門には、情報セキュリティ責任者と実務を行うセキュリティ管理者を据える組織体系が多く検討されている。

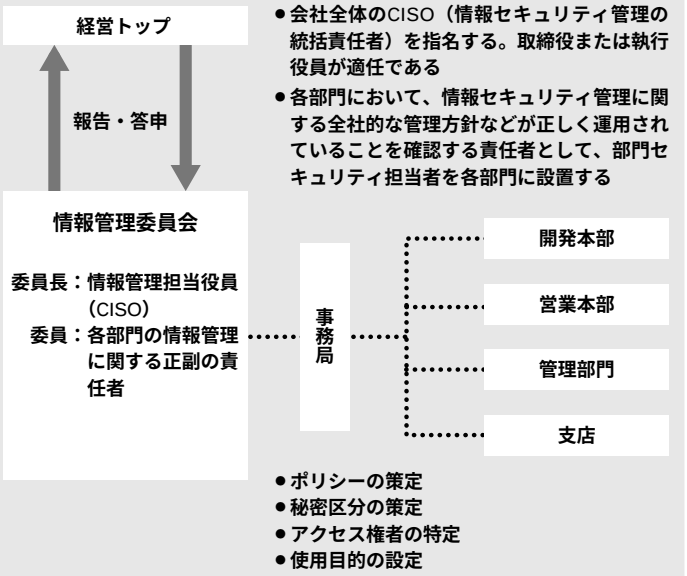
また、不正を内部告発した社員を解雇したり、左遷したりすることを禁じる公益通報者保護法が2006年４月に施行された。内部告発のルールを明確にし、企業に証拠隠滅の恐れがある場合の報道機関など外部への告発も保護対象にしている。これにより、企業は2006年４月までに、通常の指揮命令系統から独立した内部通報窓口を設けるか、弁護士事務所など外部に通じるホットラインを設けるなど、体制整備を進める必要が生じた。

ここ数年、内部告発で相次ぎ事件が発覚し、内部告発は企業の不正を暴く有効な方法として認識されている。内部告発者として従業員、派遣社員、アルバイト、退職者は保護対象者だが、取締役や監査役は保護の対象外となる。また、企業や従業員の信用失墜を狙うような「不正の目的」の場合は当然対象外であり、制度上の配慮が必要である。

（4）現場に根づいた教育の徹底

一般的な話を一方通行的に行っても、従業員一人ひとりにどれだけセキュリティ意識が残るかという問題がある。また、年１回10分程度のウェブ教育を行ったとしても同様だろう。従業員の業務のなかで、どのような情報が営業秘密で、それをどのような方法で現在管理していて、どう管理していくべきか、そのときにどういった問題があり、回避するにはどうしたらいいのかなどを部全体で議論しなければ、社員が理解することはできない。それぞれの現場によって業務プロセス、役割

図７　全社的情報管理統制組織の設置



が異なるため、業種、職種、役職などに合わせたオーダーメードの対応が必要になる。

特に、企業にとって非常に重要な営業秘密に接する可能性が高い者や、担当管理職などに対しては、より専門的な教育・研修活動を実施すべきである。担当取締役など情報の取扱責任者は、専門家などのサポートを受け、法律、システム、情報管理手法に関する知識を深めるとともに、その必要性と達成目標について、最高責任者をはじめとする経営幹部と十分話し合う必要がある。

全社的なリスクマネジメントのなかで、いかに営業秘密を管理、運用していくかは、企業責任として法律を遵守するという観点とは別に、重要な経営戦略の１つである。経営トップが責任を持って主導的に行わない限り、従業員まで浸透させることは難しい。いくらシステムやソフトウェアに多額の投資をしたとしても、無駄な投資になりかねない。

教育上重要なのは、各従業員の生活や人生にとって、故意、不用意にかかわらず、情報漏洩が生じた場合のリスクが大きいことを認識させることである。たとえば、営業成績トップの従業員がたった１回の不用意な重要書類の紛失で何もかも失ってしまうほど恐ろしいということを、イメージさせられるどうかである。経営層にとっては、末端の社員の不用意な行動で責任を負わされるリスクをどう管理するかということでもある。

（５）多面的な人事制度

ただ営業成績だけを上げればいいといった成果主義のもと、過酷な社員競争のなかで、現在まで多くの社会通念や法令遵守を無視した不正行為が生まれてきた。最近になってCSR（企業の社会的責任）の重要性が叫ばれているが、そこには、単純な業績評価だけでなく、企業価値を引き上げられる要素を加味した評価が求められる。内部監査や人事制度を変える試みを含め、実効性を持たせる評価システムが必要になってくる。

また、銀行などでは不正を防ぐ意味でも、人事異動を定期的に行っているが、技術系企業の開発系部門では状況は異なる。企業の根幹となる、競争力低下につながるような重要な技術、ノウハウの流出を避ける意味でも、出入りの激しい人事は避けるべきである。企業へのロイヤルティを高め、好条件で引き抜かれることのリスクを軽減することに努める必要がある。

3　海外進出で注意すべき点

メーカーの海外展開に伴い、多様な営業秘密の漏洩が散見される。交渉段階でビジネス機会の逸失を恐れて不利な契約を締結してしまうケース、現地の人間を教育する際に、十分に技術指導したあげく、現地の他社に転職されてしまうケースなどが少なくない。

製造技術にからむ営業秘密は、各国で法的保護を受けるよう、現地で権利化して保護を強化することも考えられる。技術管理を行うなど、相手国の知的財産保護レベルに応じた対策が求められる。知財保護体制が未整備な国へ進出せざるを得ない企業にとって、最先端技術の問題はリスクが大きく、十分検討する必要がある。国によっては、法令遵守が重要視されず、秘密保持契約の締結が全く無意味なものになる可能性もある。

よって海外進出するメーカーなどの営業秘密管理施策としては、現地の作業環境の中で

根幹の部分は造らない、見せない戦略が求められる。部品や材料には技術やノウハウが集積しているので、基幹部品は日本で製造し、モジュール化して輸出することも考えられる。また、相手先に渡す図面にはノウハウを書き込まず、キーとなる製造工程をブラックボックス化することも検討に値する。CAD/CAM（コンピュータによる設計・製造）のデータは、現地のパソコン端末で読めないようセキュリティをかけることも考えられる。コア技術を伴う製造設備は、できれば資本関係のある企業で製造することが望ましい。

たとえばシャープは、2006年10月の生産稼働を目指して、三重県亀山市に第８世代のガラス基板に対応する世界最大の大型ガラス基板採用の最新鋭工場を建設する。松下電器産業も、2007年に稼働の予定で、兵庫県尼崎市に薄型テレビのPDP（プラズマディスプレイパネル）生産のために、年500万台以上の生産能力を持つ世界最大の工場を建設する。これら薄型テレビの世界的なリーティングカンパニーは、世界的先進工場を海外ではなく、国内で運営する計画である。

今後は、コスト削減を目的にした海外進出から、多様なリスクを踏まえた海外進出への転換が求められる。

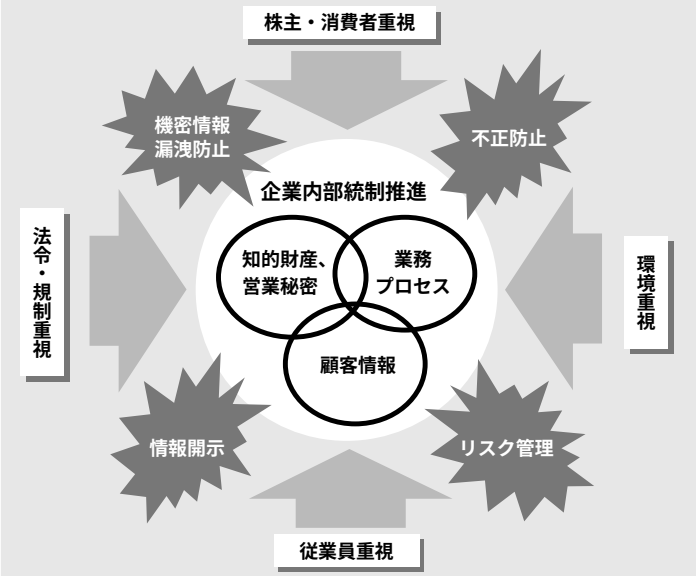
4　ステークホルダーのための経営

企業の重要な情報を管理する経営者に求められているのは、法令遵守を基本として、株主、消費者、従業員などステークホルダー（利害関係者）のための経営である。企業不祥事が発生する原因の１つは、株主を意識していないことである。株主を意識していない企業は、株主に対する法的責任を適正に果たさないケースが多い。「社会の論理」より「会社の論理」が優先される傾向にある。また、消費者への多大な迷惑を顧みず、単に営業利益を追求するという行為も経営リスクが高い。さらに、従業員を観察、管理できていないことも不正の根源になり得る。

一方で、社内の法令遵守などに対する意識の低さもある。重要書類の紛失やノートパソコンの外部での盗難はその典型である。

以上見てきた多様な法規制に対応することをよい機会として、遵法意識の強化も含め、企業、連結グループ全体の社内システムを見直すべきだと考える（図８）。

図８　企業内部統制の各要素の関係性



著者
岡野靖丈（おかのやすたけ）
経営システムコンサルティング部主任コンサルタント
専門は内部統制、リスクマネジメント、情報セキュリティ管理