資料６－２

営業秘密管理指針

平成１５年１月３０日
平成１７年１０月１２日改訂

経済産業省

目次

第１章　概説 3
１．　背景 3
２．　営業秘密の管理の意義 4
３．　指針の構成 5
第２章　不正競争防止法上の営業秘密の保護 6
１．　営業秘密の定義 6
（１）　秘密管理性（秘密として管理されていること） 7
（２）　有用性（事業活動に有用な情報であること） 8
（３）　非公知性 8
２．　営業秘密の民事的保護 9
（１）　営業秘密に係る「不正競争」の各類型 9
（２）　不正競争行為に対する措置 11
（３）　民事訴訟における営業秘密の保護（平成 16 年改正により追加） 12
３．　営業秘密の刑事的保護 13
（１）　営業秘密侵害罪の類型 13
（２）　営業秘密侵害罪に関する留意点 15
（３）　法人処罰について 16
第３章　営業秘密を保護するための管理のあり方 18
１．　概要 18
（１）　基本的な考え方 18
（２）　判例にみる秘密管理性 19
（３）　指針における具体的管理方法の記載について 20
２．　物理的・技術的管理 21
（１）　基本的な考え方 21
（２）　物理的管理 21
（３）　技術的管理 26
３．　人的管理 29
（１）　基本的な考え方 29
（２）　従業者に対する教育・研修の実施 31
（３）　従業者、退職者等に関する就業規則・契約等による秘密保持の要請 32
（４）　派遣従業者 34
（５）　転入者 34
（６）　取引先 36
４．　企業と従業者・退職者との適切な秘密保持契約の在り方 38
（１）　秘密保持契約を締結する意義 38
（２）　秘密保持契約の内容 38

（３）　秘密保持契約を締結するタイミングと事務手続き 41
（４）　企業間の秘密保持契約との関係..... 43
５．　組織的管理..... 45
（１）　自社の営業秘密の管理のための組織的管理..... 45
（２）　他社の営業秘密を侵害しないための組織的管理..... 46
（３）　望ましい管理方法..... 49
（４）　情報管理に関するマネジメント規格、個人情報保護との関係 61

第１章　概説

１．　背景

営業秘密の保護は、平成２年の不正競争防止法改正によって法律上明確に位置づけられた。昭和 40 年代に刑法改正草案において企業秘密漏示罪が検討された際には、多くの反対論の前にその実現は見送られたが、その後の国際的な事業展開の増大に伴う企業間取引の拡大により、営業秘密の保護を求める声が大きくなってきた。加えて、当時ＷＴＯの前身であるＧＡＴＴのウルグアイラウンド交渉において、知的財産の貿易的な側面について規定するＴＲＩＰｓ協定の交渉が行われ、その中で各国が営業秘密の不正使用への差止請求権を明定すべきことが議論されていた。これを受けて、平成２年の改正では、営業秘密を法律上定義するとともに、その不正取得行為等を不正競争行為と位置付け、差止請求、損害賠償請求等の対象とすることとされた。

その後、アジア諸国を中心とする生産コストの低い国における経済的な発展が我が国企業の競争力を脅かすに至り、一方で知識社会の傾向がますます強まる中で、付加価値の高い製品・サービスの供給によって利益を確保していくことが企業にとって死活問題となるに至った。そのようなビジネスモデルの前提条件となるのが、企業毎の個性であり他社と自社を差別化する能力であることから、競争力の源泉としての差別化の要素がますます重視されるようになってきた。そうした要素のうち極めて重要なものの一つが、技術やノウハウなどの知的財産であり、中でも他者には内容を開示しない営業秘密の扱いが注目されるようになっていった。

こうした状況の下、政府は、知的財産立国を目指して知的財産戦略大綱を策定（平成１４年７月）し、営業秘密の保護強化が盛り込まれた。具体的には、営業秘密の不正取得等に対する刑事罰の導入（平成 15 年の不正競争防止法改正により実現）と、「企業が営業秘密に関する管理強化のための戦略的なプログラムを策定できるよう、参考となるべき指針を 2002 年度中に作成する」ことが盛り込まれ、これを受けて、経済産業省は、産業構造審議会知的財産政策部会における審議を経て、平成 15 年 1 月に「営業秘密管理指針」を策定・公表した。

また、大学については、平成 16 年 4 月に、大学が秘密管理指針を策定する際の指針となる「大学における営業秘密管理指針作成のためのガイドライン」を作成・公表している。

その後も、東アジア諸国及び地域、とりわけ中国や韓国、台湾などの技術的な発展は加速し、営業秘密の侵害によって我が国企業の技術的優位が脅かされるリスクが増大するとともに、具体的な侵害事例も多くなってきたこと、企業におけるリストラの進展や雇用の流動化等により、退職者（元役員・元従業者）による営業秘密の侵害といった問題が顕著になってきたことなどの理由から、営業秘密の保護強化を求める声が各方面から強まった。

このような状況の下、本年（平成 17 年）の第 162 回通常国会において、国外犯の処罰、一定の条件を満たす退職者の処罰及び法人処罰の導入、刑事罰の引上げなどを内容とす

る不正競争防止法等の一部を改正する法案が成立した（平成 17 年 11 月 1 日施行）。

改正を検討する過程では、企業と退職者等との間での秘密保持契約に関して何らかの指針を示すこと、及び法人処罰に関連して法人の選任監督義務に関して何らかの指針を示すことが必要であるとの指摘があった。

また、平成 17 年 4 月の個人情報保護法の完全施行を契機として、多くの企業が自社の取り扱う情報の管理の重要性を認識し、自社が保有する情報に対する管理措置について見直しを図っているところである。

このような状況を踏まえ、経済産業省は、平成 15 年に策定した営業秘密管理指針を改訂し、企業の営業秘密の管理強化を促すこととした。各企業においては、今回改訂した本指針を参考として自らの強みを明確に認識し、戦略的に営業秘密の管理強化を図ることを通じ、的確かつ有効な経営を行っていくことを強く期待するものである。

２．　営業秘密の管理の意義

不正競争防止法については、これまで三度の改正を通じて、営業秘密の不正取得及び不正取得した営業秘密の使用又は開示に対する民事的措置及び刑事的措置の整備が図られてきた。しかし、こうした法的な措置はあくまで不測の事態が発生した場合に解決を図るための手段に過ぎず、企業による適切な管理が行われることが前提である。

その出発点は、企業が「自社にとって大事な情報を、大切に保護する」ことである。

グローバルな国際競争が激化する中、我が国が中期的にその競争力を維持していくためには、企業がそれぞれにもつ強みを維持・強化し、弱みを克服しつつ、経営・開発・生産・販売力等様々な側面で他社の追随を許さない状況を実現することが重要である。

このため、企業は、まず自らの強みを明確に認識して経営者の明確な経営哲学とリーダーシップの下でさらなる選択と集中を行い、戦略的な投資を行うとともに、そうした強みの源泉となる技術やノウハウの意図しない流出や、自らの投資の成果にただ乗りして不当な利益を得ようとする行為を防止するために自衛策を講ずる必要がある。営業秘密の保護・管理は、まさにその一環として行われるものである。

すなわち、営業秘密の管理に当たっては、自らの強みがどこにあり、その強みの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明確に認識し、その上で、実効的な管理を行うことが重要である。

また、営業秘密を適切に管理することは、不正競争防止法による営業秘密保護のための要件の１つである秘密管理性の重要な要素となるため、法的保護を受けるための前提条件である。いかに価値の高い情報であったとしても、その情報が秘密として適切に管理されていなければ、法的保護を受けることはできない。

ただし、企業の保有するできるだけ多くの情報を適切に管理することは重要であるが、多くの情報をやみくもに営業秘密として管理しようとすることは、管理コストを高めるとともに管理の実効性を低下させることとなり、結果的に秘密管理性が認められなくなることにもなりかねない。

このため、企業は、営業秘密として管理すべき情報を、経営上の重要性や有用性を踏まえて絞込む必要がある。

あわせて、営業秘密侵害罪への両罰規定の導入をはじめとして、犯罪を行った行為者のみならず、その者が所属する企業の責任が問われる場面が増加しつつある。企業は、自社の情報を保護するのみならず、他社から預かった営業秘密も保護する、あるいは他社の営業秘密の不正取得等を防止することにも留意しなければならない。

つまり、コンプライアンスが重視される時代において企業は「自社の従業者が、他社の営業秘密を侵害しない」ための管理を行うことの必要性が、自社の営業秘密の漏洩防止の必要性とともに増大している。

これら２つの観点からの管理を実効的に行うためには、情報や媒体自体を物理的に管理することに加えて、営業秘密を扱う「人」の管理を行うことが重要である。

「人」の管理において、罰則などで威嚇しながら全ての役員・従業者の動向をいたずらに厳格に管理するような管理手法は、通常の事業活動を行う者を萎縮させ、情報の共有による生産性向上や円滑な事業活動の促進を妨げるだけではなく、かえって管理が非効率になる場合がある。むしろ、管理の実効性を向上させるためには、誰がどの情報にアクセス権限を有しているかを正しく把握し、重要な情報を知っている者を大切にすることにより、企業に対する満足度や一体感を高め、企業と従業者等が協力しながら、営業秘密管理に対する共通の意識を持ち、自社の営業秘密の漏洩や他社の営業秘密の侵害を起こさないよう、組織として取り組むことが重要である。

３．　指針の構成

本指針においては、本章において全般的な概観を行った上で、第２章において不正競争防止法における営業秘密に関する部分につき説明し、第３章において、各企業における営業秘密の実効的な管理方策について述べている。

第２章　不正競争防止法上の営業秘密の保護

１．　営業秘密の定義

「営業秘密」とは、①秘密として管理されていること、②有用な情報であること、③公然と知られていないことの3つの要件を満たす技術上、営業上の情報である。

不正競争防止法上の営業秘密の保護については、同法上の「営業秘密」の定義を満たすものが、その対象となり得る。

同法第 2 条第 6 項は、営業秘密を「秘密として管理されている〔①秘密管理性〕生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報〔②有用性〕であって、公然と知られていないもの〔③非公知性〕をいう。」と定義しており、この３つの要件全てを満たすことが同法に基づく保護を受けるために必要である。

したがって、同法上の「営業秘密」は、国から事務の委任を受け、秘密保持義務を課された機関等が、当該事務に関して「知り得た秘密」や、労働者派遣事業の適正な運営の確保及び派遣労働者の就業条件の整備等に関する法律（以下、「労働者派遣法」という。）（同法第 24 条の 4）に規定される「その業務上取り扱つかったことについて知り得た秘密」とは必ずしも一致しない。

以下、上記３要件について説明する。

（１）秘密管理性（秘密として管理されていること）

「秘密管理性」が認められるためには、その情報を客観的に秘密として管理していると認識できる状態にあることが必要である。
具体的には、①情報にアクセスできる者を特定すること、②情報にアクセスした者が、それが秘密であると認識できること、の2つが要件となる。

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。

これまでの裁判例では、①当該情報にアクセスできる者を制限するとともに、②同情報にアクセスした者にそれが秘密であることが認識できることが必要とされている（東京地裁平成 12 年 9 月 28 日）。

営業秘密の管理主体は、事業者であることが前提である（第 2 条第 1 項第 7 号）ため、その情報の創作者が誰であるかを問わず、事業者が当該情報を秘密として管理している場合には「営業秘密」になる可能性がある。

したがって、

a） 情報が事業者によって秘密として管理されていれば、非常に記憶力が良い人がその情報を記憶して持ち出した場合においても、当該記憶されて、持ち出された情報は営業秘密に該当する

b） 従業者等（役員・従業者）が創作した情報であっても、単にその従業者等の頭の中に留まり、事業者が秘密として管理していない情報については、営業秘密とはならない

c） 従業者等が、在職中に創作した情報であっても、その情報を事業者が営業秘密として管理している場合には、その不正な使用又は開示行為は処罰や差止めの対象となり得る

d） 技能・設計に関して従業者等が体得したノウハウやコツなどについても、事業者が秘密として管理しているものであれば営業秘密となり得るが、事業者によってそのような管理がなされていなければ、営業秘密には該当しない。このため、個人に身に付いた技能のように管理することが難しいものは、一般的には営業秘密になりにくい

と考えられる。

一方、（形式的に）社内秘として扱われている情報が全て営業秘密に該当する訳ではない。例えば、徒らに「秘」のスタンプを押印したような場合においては、それが実質的にアクセス制限が行われていないという理由で、あるいは客観的に（本当に何が重要な秘密であるかについての）認識可能性がないという理由で、営業秘密の条件としての秘密管理性が認められないものと解される可能性が高い。また、徒らに元々「秘」と印刷された紙を使って情報を多数の人に回付するような場合も同様に解される可能性が高い。

（２）有用性（事業活動に有用な情報であること）

「有用性」が認められるためには、その情報が客観的に有用であることが必要である。
しかし、企業の反社会的な行為などの公序良俗に反する内容の情報は、「有用性」が認められない。

有用性についても、保有者の主観によって決められるものではなく、客観的に有用である必要がある。

この有用性とは、競争優位性の源泉となる場合を含め、そもそも当該情報が事業活動に使用されたり、又は使用されることによって費用の節約、経営効率の改善等に役立つものであることを意味し（事業への活用性）、例えば、「財やサービスの生産、販売、研究開発に役立つ等事業活動にとって有用なもの」であることが必要とされる（東京地裁平成 14 年 2 月 14 日）。直接ビジネスに活用されている情報に限らず、間接的な（潜在的な）価値がある場合も含み、例えば、いわゆるネガティブ・インフォメーション（ある方法を試みてその方法が役立たないという失敗の知識・情報のこと）にも有用性は認められる。

現在の事業に活用できる情報だけなく、将来（近未来も遠い未来も含む）の事業に活用できる情報にも有用性が認められ得るが、同じ情報でも、例えば試験段階か、製造段階かによって、有用性の有無がかわる場合もあり得る。

一方、公序良俗に反する内容の情報は、その内容が社会正義に反し、秘密として保護されることに正当な利益がある情報とはいえないので、有用性はないと判断される。（上記裁判例は、「犯罪の手口や脱税の方法を教示し、あるいは麻薬・覚せい剤等の禁制品の製造方法や入手方法を示す情報のような公序良俗に反する内容の情報は、法的な保護の対象に値しないものとして営業秘密として保護を受けないものと解すべきである」と判示している。）

（３）非公知性

「非公知性」が認められるためには、保有者の管理下以外では一般に入手できないことが必要である。

非公知性が認められるためには、当該情報が刊行物に記載されていない等、保有者の管理下以外では一般に入手できない状態にあることが必要である。

具体的には、書物、学会発表等から容易に引き出せることが証明できる情報は、非公知とは言えない。他方、人数の多少にかかわらず、当該情報を知っている者に守秘義務が課されていれば、非公知と言える。さらに、同じ情報を保有している者が複数存在する場合であっても、各自が秘密にしている等の事情で当該情報が業界で一般に知られていない場合には、非公知であるものと考えられる。

２．　営業秘密の民事的保護

不正競争防止法では、営業秘密の不正な取得･使用･開示行為を類型ごとに列挙してそれを「不正競争」と定義し、民事訴訟において差止め、損害賠償、信用回復措置を請求することを可能としている。
また、民事訴訟の場で証拠に含まれる営業秘密が公開されてしまうのを防ぐために、秘密保持命令や、裁判の公開停止などの制度等が特別に設けられている。

（１）営業秘密に係る「不正競争」の各類型

不正競争防止法では、第 2 条第 1 項第 4 号～第 9 号において、営業秘密に係る行為を列挙して、それらを「不正競争」と定義している。

これらの「不正競争」は、最初に営業秘密を保有者から不正に取得した場合と、最初に営業秘密を保有者から正当に取得した場合に分類することができる。

①　第 4 号

保有者から、営業秘密を窃取等の不正の手段により、取得しようとする行為（以下、「不正取得行為」という。）及び取得後に使用し、又は開示する行為である。

例えば、従業者が会社の保管する大口受注報告書等の機密文書を窃取し、産業スパイに開示する行為（東京地裁昭和 40 年 6 月 26 日）がこれにあたる。

②　第 5 号

第 4 号の不正取得行為の介在について悪意・重過失の転得者の取得行為及び、その後の使用し、又は開示する行為である。

例えば、会社の機密文書を窃取した従業者から、産業スパイが当該機密文書を受け取る行為等がこれに当たる。

③　第 6 号

第三者が不正取得行為の介在について善意・無重過失で営業秘密を取得しても、その後悪意・重過失に転じ、その営業秘密を使用し、又は開示する行為である。

例えば、営業秘密を取得した後に、産業スパイ事件が大々的に報道されて不正取得行為が介在していた事実を知りながら、営業秘密を使用し、又は開示する行為がこれに当たる。（ただし、適用除外規定の適用があり得る）。

④　第 7 号

営業秘密の保有者が従業者、下請企業、ライセンシー等に対して営業秘密を示した場合に、その従業者等が、不正の競業その他の不正の利益を得る目的又は営業秘密の保有者に損害を加える目的で、その営業秘密を使用し、又は開示する行為である。

「競業の目的」とは、競争関係にある事業を行う目的をいい、例えば、通信販売業を営む企業の取締役が、在職中に同業の会社を設立した上、元の企業の従業者に顧客名簿を持ち出させて、当該名簿を使用して通信販売業を行った行為（大阪高裁

昭和 58 年 3 月 3 日）等がこれに当たる。

⑤　第 8 号

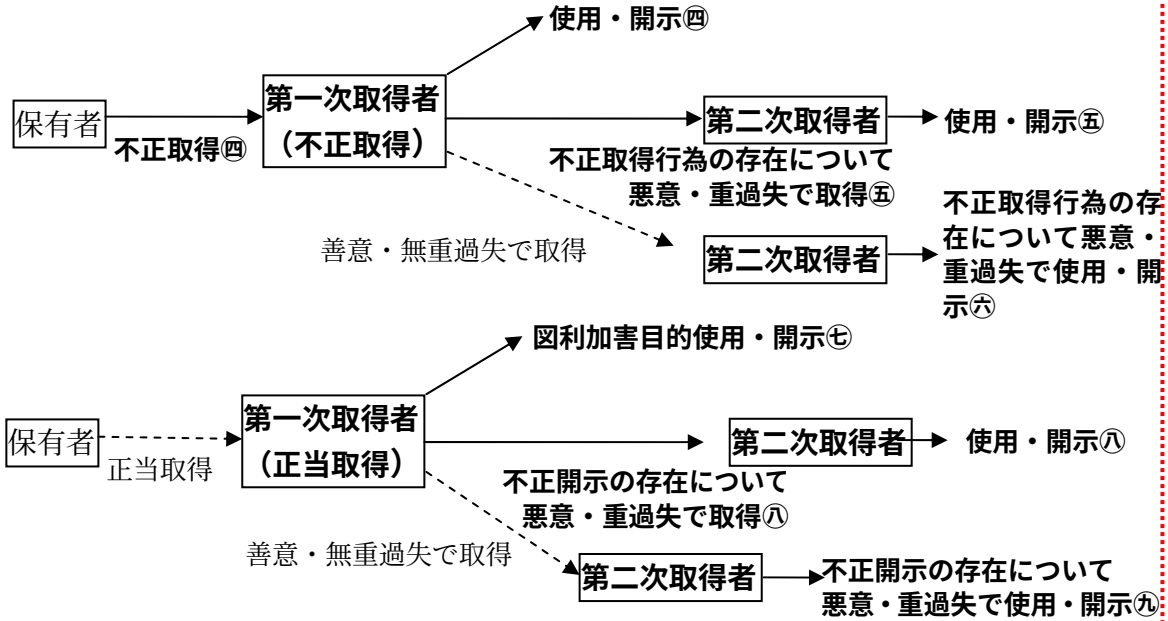
営業秘密を取得する際に、第 7 号に規定する不正開示行為若しくは守秘義務違反による開示行為によるものであること、若しくはそのような不正開示行為が介在したことについて悪意・重過失で営業秘密を取得する行為、その取得した営業秘密を使用し、又は開示する行為である。

例えば、ロボットメーカーの従業者が、在職中に同種の営業を営む企業の設立に参画し、退職時に元の企業から無断で持ち出したロボット製造技術に関するノウハウ等を開示した一連の行為が不法行為責任を負うとされた事例（東京地裁昭和 62 年 3 月 10 日）は、第 7 号に該当する事例と考えられるが、新会社側も当該従業者がそのノウハウに関して機密保持義務を負っていることを知りながら、機密漏洩行為をさせて使用しているため、こうした行為は本号の「不正競争」に当たる。

⑥　第 9 号

第三者が、営業秘密を取得した後に、その取得が不正開示行為によるものであったこと、若しくは不正開示行為が介在したことについて悪意・重過失で、その営業秘密を使用し、又は開示する行為である。

例えば、営業秘密を取得した後に、保有者から警告を受けて不正開示行為が介在していた事実を知りながら、営業秘密を使用し、又は開示する行為がこれに当たる（ただし、第 6 号と同様に、適用除外規定の適用があり得る）。



※〇囲いの漢数字は、不正競争防止法第2条第1項の各号の「不正競争」に該当することを意味する。
「不正開示」＝「図利加害目的開示」又は「法律上の義務違反による開示」
悪意・重過失＝当該行為があったことを知っている、あるいは重大な過失なくして知らないこと。
善意・無重過失＝当該行為があったことを、重大な過失によらずに知らないこと。

（2）不正競争行為に対する措置

①　差止請求権（第 3 条・第 15 条）

「営業上の利益を侵害され、又は侵害されるおそれが生じたこと」を要件に、侵害の停止又は予防に加えて、侵害の行為を組成した物の廃棄、侵害の行為に供した設備の除却その他侵害の停止又は予防に必要な行為を請求することができる。

営業秘密に係る不正使用行為に対する差止請求権は、当該行為が継続する場合においては、当該行為及びその行為者を知ったときから 3 年の消滅時効と、当該行為の開始時から 10 年の除斥期間が設けられている。（第 15 条）

②　損害賠償請求権（第 4 条～第 9 条）

「故意又は過失」により「営業上の利益を侵害」されたことを要件に、損害賠償を求めることができる。

損害賠償の請求を行う場合、損害額はその請求を行う被害者側が立証しなければならないが、営業秘密に係る不正競争の場合、侵害した者が営業秘密侵害行為を通じて得た利益の額を立証すれば、その利益の額が被害者の損害額と推定される。（第 5 条第 2 項）

特に、技術上の営業秘密が侵害された場合には、特別に、（被害者がその侵害行為がなければ販売することができた物の単位数量当たりの利益）×（侵害者が販売した物の数量）を損害額と推定することが可能であり、侵害者が利益を上げていない場合や侵害者の利益額が小さい場合の逸失利益の立証が容易になる。（第 5 条第 1 項：平成 15 年改正により追加）

③　信用回復措置請求権（第 14 条）

「故意又は過失」により信用を害された場合は、謝罪広告等の営業上の信用を回復するのに必要な措置を求めることができる。

（３）民事訴訟における営業秘密の保護（平成 16 年改正により追加）

営業秘密侵害に対する損害賠償請求を行う場合、裁判所の求めに応じ、準備書面や証拠等を提出する必要がある。（第 7 条第 1 項）

しかし、これらの準備書面や証拠等に営業秘密が含まれる場合には、訴訟の場で営業秘密が漏洩するのを恐れ、提出が困難になる場合もある。このため、訴訟における営業秘密を保護するために次のような措置が導入されている。

①　秘密保持命令（第 10 条～第 12 条）

裁判所は、訴訟の当事者等に対し、準備書面又は証拠に含まれる営業秘密を使用し、又は開示してはならない旨を命ずることができる。（秘密保持命令）

秘密保持命令に違反して営業秘密を使用し、又は開示した場合には、5 年以下の懲役又は 500 万円以下の罰金（またはその両方）が科される。

また、秘密保持命令が発せられた訴訟に係る訴訟記録について、民事訴訟法第 92 条第 1 項の決定があった場合において、当事者から同項に規定する秘密記載部分の閲覧等の請求があり、かつその請求の手続きを行った者が当該訴訟において秘密保持命令を受けていない者であるときは、裁判所書記官は、同項の申し立てをした当事者に対し、その請求後直ちに、その請求があった旨を通知しなければならない。

②　書類の提出等（インカメラ審理）（第 7 条第 2 項、第 3 項）

裁判所から必要な書類の提出を求められた場合、その書類の所持者は、正当な理由がある場合には提出を拒否することができる。この「正当な理由」に該当するか否かについては、訴訟の当事者や訴訟代理人等にのみに書類を開示した上で意見を聴き（いわゆるインカメラ審理)、裁判所が判断することとなっている。

③　営業秘密が問題となる訴訟における公開停止（第 13 条）

営業秘密侵害に係る訴訟については、営業秘密に該当するものについて当事者等が当事者本人又は証人等として尋問を受ける場合には、裁判官の全員一致により、当該事項の尋問の公開を停止することができる。

３．　営業秘密の刑事的保護

不正競争防止法は、営業秘密の不正取得･使用･開示行為のうち、一定の行為について、5 年以下の懲役又は 500 万円以下の罰金（又はその両方）を科すこととしている（営業秘密侵害罪）。
日本国内で管理されている営業秘密については、日本国外で不正に使用･開示した場合についても処罰の対象となる。
いずれの行為も、「不正の競争の目的」で行う行為が刑事罰の対象であり、報道、内部告発の目的で行う行為は刑事罰の対象とはならない。
なお、営業秘密侵害罪は、犯罪被害者保護の見地から、親告罪（被害者による告訴がなければ公訴を提起することができない）とされている。

（１）営業秘密侵害罪の類型

不正競争防止法第 21 条第 1 項第 4 号から第 9 号までにおいて、営業秘密侵害罪に該当する６つの類型を規定している。

①　第 4 号

営業秘密を不正取得した後、これを不正の競争の目的で使用し、又は開示する罪

②　第 5 号

第 4 号の使用又は開示の用に供する目的で、営業秘密が記録された媒体を取得し、又は複製することにより、その営業秘密を不正に取得する罪

③　第 6 号

営業秘密を示された者が、不正の競争の目的で、その営業秘密が記録された媒体を不正に領得し、又は複製して、その営業秘密を使用し、又は開示する罪

④　第 7 号

営業秘密を示された役員又は従業者が、不正の競争の目的で、その営業秘密を使用し、又は開示する罪

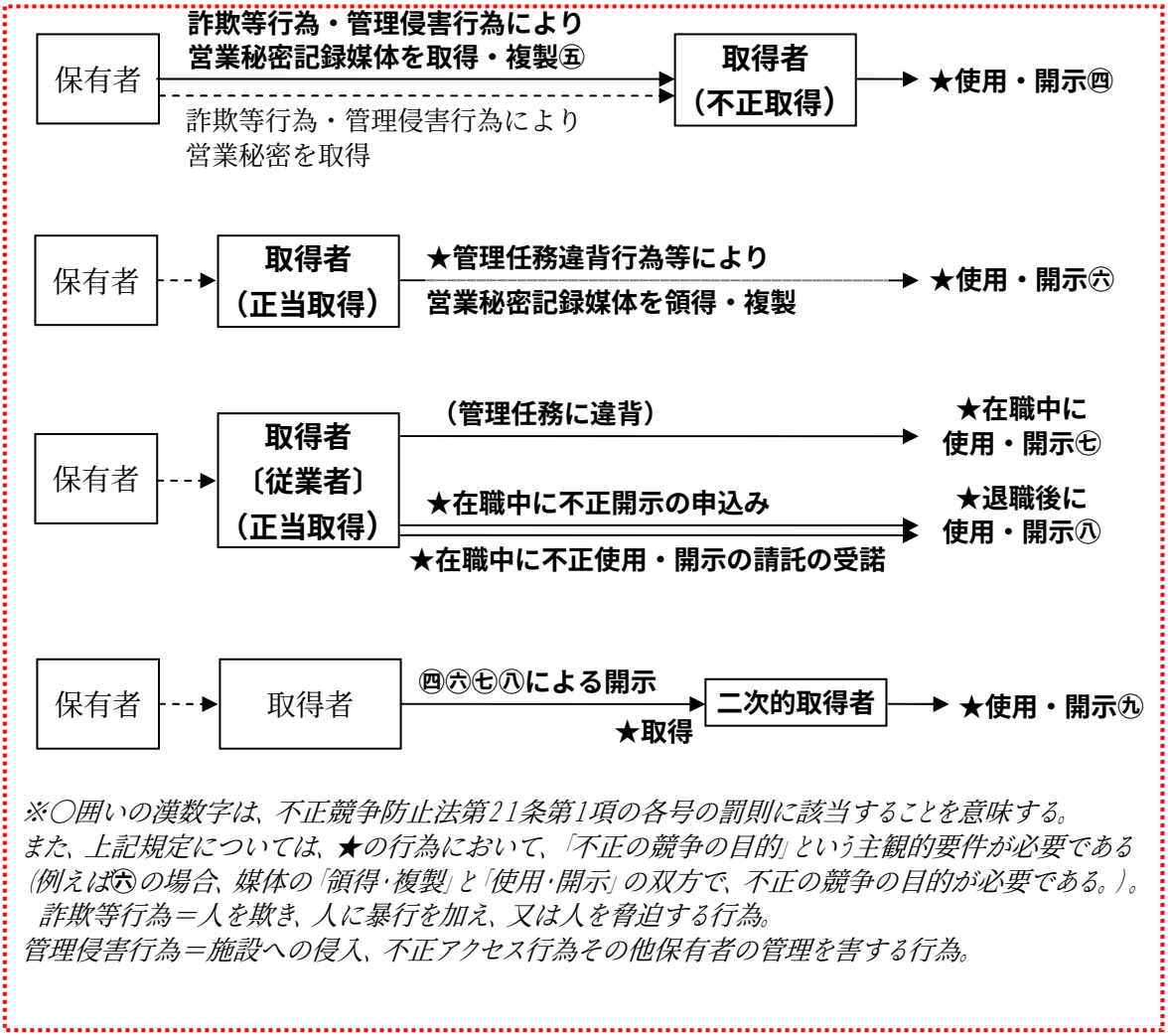
⑤　第 8 号（平成 17 年改正により追加。同年 11 月 1 日施行。）

営業秘密を示された役員又は従業者であった者が、不正の競争の目的で、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、その営業秘密を退職後に使用し、又は開示する罪

⑥　第 9 号（平成 17 年改正により追加。同年 11 月 1 日施行。）

不正の競争の目的で、上記①③④⑤の罪に当たる開示によって営業秘密を取得して、その営業秘密を使用し、又は開示する罪

なお、第 7 号及び第 8 号の「従業者」には、使用者と労働契約関係のある労働者のみならず、労働者派遣法に基づく派遣労働者が含まれる。



※〇囲いの漢数字は、不正競争防止法第21条第1項の各号の罰則に該当することを意味する。
また、上記規定については、★の行為において、「不正の競争の目的」という主観的要件が必要である（例えば㉖の場合、媒体の「領得・複製」と「使用・開示」の双方で、不正の競争の目的が必要である。）。
詐欺等行為＝人を欺き、人に暴行を加え、又は人を脅迫する行為。
管理侵害行為＝施設への侵入、不正アクセス行為その他保有者の管理を害する行為。

（２）営業秘密侵害罪に関する留意点

①　主観的要件

処罰範囲を明確に限定するため、各号毎に違法性を基礎付ける目的要件が付されている。具体的には「不正の競争の目的」と規定されているが、これは自己を含む特定の競業者を競争上優位に立たせるような目的を意味し、報道目的や内部告発目的などは、一般的にこれには該当しない。

第９号については、取得の時点から、不正の競争の目的が存在することが要件となっている点に注意が必要である。

②　国外犯（平成 17 年改正により追加。同年 11 月 1 日施行。）

営業秘密については、詐欺等行為若しくは管理侵害行為が行われた際に日本国内で管理されていたもの、又は営業秘密の保有者から正当に示された際に日本国内で管理されていたものについては、日本国外で不正使用又は開示が行われた場合についても、日本国内で不正使用又は開示が行われた場合と同様に処罰の対象となる。

③　親告罪

営業秘密侵害罪は被害者等の告訴があって、はじめて罪に問われることとなる（親告罪）。これは、被害者が刑事裁判を望まないにもかかわらず公判手続が開始されることにより、営業秘密がその過程でさらに開示されることを避けるためである。

④　罰則（平成 17 年改正により引き上げ。同年 11 月 1 日施行。）

営業秘密侵害罪の罰則は、5 年以下の懲役又は 500 万円以下の罰金であり、懲役刑と罰金刑を併せて科すことができる。

また、平成 17 年改正により、自らがアクセスする権限を持たない営業秘密を不正に取得し、又は、その上で使用又は開示した場合（第 21 条第 1 項第 4 号、第 5 号、第 9 号違反）、その者を罰するほか、両罰規定により、その行為者が所属する法人等に 1 億 5 千万円以下の罰金が科されることとなった。（法人処罰については、「（３）法人処罰について」を参照。）

（３）法人処罰について

営業秘密にアクセスする権限のない者が、業務に関して営業秘密侵害罪を犯した場合、その行為者自身が処罰されるだけでなく、法人に対しても罰金刑が科され得る。

法人が免責されるためには、積極的、具体的に営業秘密侵害行為を防止するために必要な注意を尽くしたことが要求される（過失推定）。

①　両罰規定について

不正競争防止法第 22 条の規定により、法人[1]の代表者、代理人、使用人、その他の従業者が、当該法人の業務に関して営業秘密侵害罪を犯した場合には、行為者自身が処罰されるだけでなく、その法人に対しても罰金刑が科され得る。

②　法人処罰が適用される行為について

営業秘密侵害罪についての両罰規定の対象は、以下に掲げる行為である。

- 法人の役員・従業者等が、その法人の業務に関し、「詐欺等行為」又は「管理侵害行為」により営業秘密を取得して不正の競争の目的で、その営業秘密を使用し、又は開示する行為（第 21 条第 1 項第 4 号）
- 法人の役員・従業者等が、その法人の業務に関し、不正の競争の目的で、「詐欺等行為」又は「管理侵害行為」により、営業秘密記録媒体等を領得し、又は営業秘密記録媒体等の記録の複製を作成する行為（同項第 5 号）
- 法人の役員・従業者等が、その法人の業務に関し、不正の競争の目的で営業秘密を開示する行為（同項第 4 号及び第 6 号ないし第 8 号）の相手方となって営業秘密を取得して、不正の競争の目的で使用し、又は開示する行為（同項第 9 号）

上記の類型はいずれも、本来その営業秘密にアクセスする権限のない者による行為である。

一方、それ以外の行為（同項第 6 号ないし第 8 号）については両罰規定の対象とはならない。

これらのうち、特に注意が必要なのは、同項第 8 号（在職中に営業秘密の開示の申込み、又は使用若しくは開示について請託を受けた（以下、約束という。）後に退職した者による使用又は開示）の相手方となって営業秘密を取得して、それを使用又は開示した場合（同項第 9 号）である。

例えば、中途採用者 a が、転職前の企業 A の営業秘密を、転職先企業 B に以前より在職している b に唆されて開示し、その開示により営業秘密を取得した b が営業秘密を不正使用する場合が考えられる。

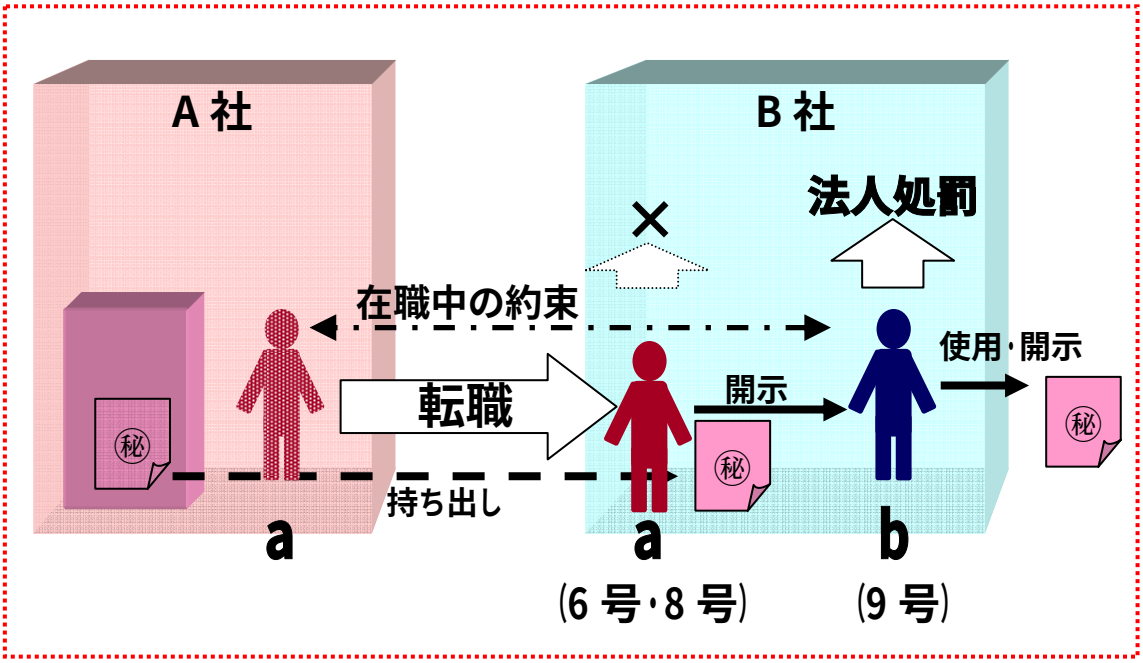
この場合、中途採用者 a の行為は第 21 条第 1 項第 6 号（媒体の領得・複製後の開

[1] 個人事業主の場合にも両罰規定は適用される。ただし、罰金刑の上限は 500 万円である。

示）あるいは第 8 号（約束後に退職した者による開示）に該当する可能性がある。第 6 号及び第 8 号は共に両罰規定の対象外であるので、中途採用者 a の行為に対する、転職先企業 B への両罰規定の適用はない。

一方、以前より在職している b については、第 21 条第 1 号第 9 号に該当し得る。第 9 号については両罰規定の対象であるので、 b の行為に対する、企業 B に対する両罰規定の適用はあり得る（次図）。

この場合において、中途採用者 a の転職に際し、営業秘密の開示等の約束の相手方となった者と、実際に開示を受ける企業Ｂの従業者が同一人物である必要がない。



③　法人に対する過失の推定

法人処罰の規定については、過去の最高裁判例によれば、法人の行為者たる従業者等の選任・監督その他違反行為を防止するために必要な注意を尽くさなかった過失の存在を推定し、その『注意を尽したことの証明がなされない限り、事業主もまた刑責を免れ得ないとする法意』であることを判示している（最高裁 昭和 40 年 3 月 26 日）。

これは不正競争防止法の規定に関するものではないが、同法においても、両罰規定について無過失免責が肯定されるためには、一般的、抽象的な注意を与えたのでは足りず、積極的、具体的に違反防止のための指示を与えるなど、違反行為を防止するために必要な注意を尽くしたことが要求されると考えられる。

このため、企業が責任を免れるためには、自社の従業者等による営業秘密侵害行為を適切に防止できるよう選任監督に関して注意を尽くしたと言えるような企業としての取組みが必要になる。（この点に関する具体的な管理措置については、「第３章５．（２）他社の営業秘密を侵害しないための組織的管理」を参照。）

第３章　営業秘密を保護するための管理のあり方

１．　概要

営業秘密の管理は、企業が自らの利益のために、管理の対象とすべき情報・人を明確に認識しつつ、形式ではなく、実効性を重視して行うものであるが、どのような保護、成果を求めるかによって、それに必要な管理の水準は異なる。

本章では、不正競争防止法による民事的保護を受けることを可能とする「ミニマムの水準」を裁判例を整理することを通じて示唆しつつ、情報自体の物理的・技術的管理、取り扱う人の管理、さらには他社情報の不正な取得・使用の防止等を含め、これら管理をシステムとして行うための組織的管理について、望ましい水準を含めて示す。

（１）基本的な考え方

企業が、競争力を維持・強化していくためには、自らの強みの源泉となる技術やノウハウが意図せず流出することを防いだり、自社の投資の成果にただ乗りして不当に利益を得ようとする行為を防いだりするために自衛策を講ずることが重要である。営業秘密の保護・管理は、まさにその一環として行われるものである。したがって、管理の形式が重要なのではなく、実効的管理が行われているかどうかがポイントとなる。

企業が、そのような認識を持たずに、ただ漠然と営業秘密管理に取り組んだ場合には、管理の対象とするべき情報も人も明確にならず、実効的な管理を行うことはできず、結果的にその情報が不正競争防止法上の営業秘密と認められないことにもなり得る。

管理の対象となる情報、人についての明確な認識があれば、実効的な管理が可能になり、管理のための過大なコスト負担を避けつつ、経営上のリスクを回避することが可能になる。

一方で、こうした情報や人を特定する管理方法は、それを厳格にすることに一定のコストを要することは事実であり、どの程度の保護を求めるのか、すなわち、一般的に有効な契約に基づく保護なのか、不正競争防止法上の「営業秘密」としての保護なのか、現実に漏洩のリスクが極めて小さいという理想的な状態を求めるのかによって、必要となる特定や管理の程度は異なる点に注意する必要がある。

また、管理に当たっては、その情報自体を管理すること、それを扱う人を管理することが、まずは重要であるが、人の要素については、「管理」といういわば企業の側の視点だけではなく、企業と従業者等とが共通の認識の下で重要な情報を扱っていくという考え方を浸透させるという視点を持つことも重要である。

その上で、そうした情報自体や人の管理を実効的に運用し、問題が生じた場合には的確に対応していくための組織的な管理を一種のシステムとして確立することが必要である。

このため、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。

なお、平成１７年の不正競争防止法の改正においては、国外犯処罰及び退職者処罰が導入された。

営業秘密が国内で漏洩する場合でも海外で漏洩する場合でも、また、漏洩の主体が現職の従業者でも退職者でも、企業側が的確な管理を行っていなければならないことに変わりはない。

しかしながら、海外での漏洩の場合、証拠の多くが日本国外に存在すると考えられることから、民事訴訟や刑事罰による解決は国内での漏洩より難しくなる。こうした場合には、その情報自体を営業秘密として的確に管理することに加え、退職者処罰の要件となっている、営業秘密の不正開示の「申込み」や「請託」の立証を容易にするためには、出張記録・残業記録の精査、秘密情報が保管されているコンピュータへのログイン回数の記録など、証拠を把握するための自助努力を行うことが重要になる。

すなわち、営業秘密の管理にあたっては、営業秘密の漏洩防止という観点とともに、万が一営業秘密が漏洩してしまった場合に、その解決を容易にするという観点も必要であり、そのためには、単に秘密管理性を維持するだけに留まらない、一層の管理努力が求められるのである。

（２）判例にみる秘密管理性

営業秘密に関する裁判例のうち、秘密管理性について判断していると考えられるものは 49 件ある。その中で、一部でも秘密管理性を肯定したものは 14 件であり、厳格な秘密管理性が要求される。これまでの裁判例においては、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。

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。

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）

これらについて、より詳細に分析すれば

Ａについては、

- アクセス権者の限定（大阪高裁平成 14 年 10 月 11 日、東京地裁平成 16 年 5

月 14 日）

- 施錠されている保管室への保管（東京地裁平成 11 年 7 月 23 日）
- 事務所内への外部者の入室の禁止（東京地裁平成 16 年 5 月 14 日、大阪高裁平成 17 年 2 月 17 日）
- 電子データの複製等の制限（大阪高裁平成 17 年 2 月 17 日）
- コンピュータへの外部者のアクセスの防止措置（東京地裁平成 16 年 5 月 14 日、大阪地裁平成 15 年 2 月 27 日）及びその実効的な実施（東京地裁平成 15 年 5 月 15 日）
- システムの外部ネットワークからの遮断（東京地裁平成 17 年 6 月 27 日）

Ｂについては、

- 「秘」の印の押印（東京地裁平成 12 年 9 月 28 日、東京地裁平成 17 年 6 月 27 日）
- 社員が秘密管理の責務を認知するための教育の実施（大阪高裁平成 14 年 10 月 11 日、東京地裁平成 16 年 5 月 14 日）
- 就業規則における秘密保持義務についての明確な規定（東京地裁平成 11 年 7 月 23 日、東京地裁平成 17 年 2 月 25 日）
- 誓約書や秘密保持契約による責務の設定（京都地裁平成 13 年 11 月 1 日、東京地裁平成 17 年 6 月 27 日）

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（東京地裁平成 11 年 7 月 23 日）
- 外部からのアクセスに関する応答に関する周到な手順の設定（大阪地裁平成 14 年 10 月 11 日）

などを判断の材料としている。

それぞれの企業の規模や組織形態、情報の形態等の状況により、これらの要素のうち不可欠な要素は異なり、したがって、これらのすべての要素を満たさなければ秘密管理性が否定されるというものでもないが、裁判例では、営業秘密の管理についての肯定的な要素の積み重ねが秘密管理性の認定につながっている（大阪高裁平成 14 年 10 月 11 日）。

一方、これらの要素の一つでも満たせば秘密管理性が認められるというものでもなく、肯定的な要素もあるが否定的な要素もある場合においては、秘密管理性が否定されたものもある（大阪地裁平成 14 年 9 月 26 日）。

（３）指針における具体的管理方法の記載について

具体的管理方法としては、物理的・技術的管理、人的管理があり、それらが実効的にシステムとして機能していくための組織的な管理がある。以下に詳述する。

２．　物理的・技術的管理[2]

（１）基本的な考え方

情報管理に当たっては、一般的には秘密情報をその他の情報から区分し、それに対する権限なきアクセスを防ぐとともに、権限に基づきアクセスした者が、その秘密の性格を認知して対応すること、営業秘密のレベルに応じた管理を行うことが必要である。

（２）物理的管理

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。

【判例の動向】

「情報の区分と表示」に関しては、秘密として扱われるべきことが明らかとなるような表示の存在について判示しているものがある。

秘密管理性を認めたものとしては、**顧客名簿が記録されている大学ノートの表紙にマル秘の印を押捺している例**（大阪地裁平成 8 年 4 月 16 日）、**情報が記録されている書面に「秘」の印が押印されている例**（東京地裁平成 17 年 6 月 27 日）等がある。

一方、秘密管理性を認めなかったものとして、**特段機密事項である旨を示す表示はなされていなかった事案について、宣誓書や就業規則の記載をもって、本件情報が秘密として管理されていたというためには、単に本件情報がきわめて重要であり、性質上『機密』に該当するというだけでは足りず、原告が、現実に、本件情報が『機密』に当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た例**（大阪地裁平成 12 年 7 月 25 日）、**各図面に、秘密として扱われるべきことが明らかとなるような印等は付されていなかった例**（大阪高裁平成 17 年 2 月 17 日）等がある。

次に、「アクセス権者の特定」については、企業の規模・業種等にもよるが、秘密情報にアクセスできる者を特定した上で、アクセスできる従業者の人数等を限定していることについて判示しているものがある。

秘密管理性を認めたものとしては、書類の**管理責任者が総務事務担当 2 人に限定されており、営業社員がこれらの書類を自由に見られないようにするとともに**、派遣就業情報を集中管理しているオフコンについても、**総務事務担当の社員が（鍵を）保管しており、それ以外の**

[2] 「物理的・技術的管理」とは、国内における情報管理に関するマネジメント規格である ISMS 認証基準 Ver.2.0 (http://www.isms.jipdec.jp/) 附属書「詳細管理策」では、「7. 物理的及び環境的セキュリティ」に相当するものである。

者がオフコンを起動させることはできないようにしていた例（大阪高裁平成 14 年 10 月 11 日）、**データベースの管理者を、原則としてコンピュータ管理を担当する1名の従業者に限定していた例（**東京地裁平成 16 年 5 月 14 日）、顧客情報について、紙に印字する場合は、**販売担当役員及び情報管理室担当役員の押印を得た上で、情報管理室の操作担当者に作業依頼するようにしているとともに、出力の操作手続を知る者は 3 名のみとしていた例（**東京地裁平成 11 年 7 月 23 日）等がある。

一方、秘密管理性を認めなかったものとして、**書式等の収められたフロッピーディスクについて特段の措置は採られていなかった例**（東京地裁平成 12 年 9 月 28 日）等がある。

次に、「媒体の保管と廃棄」に関しては、アクセス権者以外の者がアクセスできない金庫等に保管する、あるいは（実際に）鍵のかかった引き出しに保管されていることについて判示している。

秘密管理性を認めたものとしては、**印字された顧客名簿を、施錠されている保管室に保管する**とともに、**7 年経過後に、原告従業者立会いの下に、専門業者に焼却を依頼するようにしていた例**（東京地裁平成 11 年 7 月 23 日）、**文書廃棄の際に、文書廃棄の専門業者と機密保持契約を締結し、各書面の廃棄を委託していた例**（東京地裁平成 16 年 5 月 14 日）等がある。

一方、秘密管理性を認めなかったものとして、**治験データ及び輸入申請書等の紙媒体が、原告の施錠可能な引出し式のキャビネットの中に保管され**ていたが、**勤務時間中は施錠されていなかった例**（東京地裁平成 12 年 9 月 28 日）、**登録申請書が、鍵も掛けていない棚や、出窓や段ボール箱に入れられて無造作に置いてあった例**（東京地裁平成 16 年 9 月 30 日）等がある。

最後に「施設の管理」に関しては、秘密が保管されている場所の施錠の有無、あるいは秘密が保管されている場所を、その他の場所と区切っているか等について判示している。

秘密管理性を認めたものとして、**事務所内に外部の者が訪れた場合には、受付において応対し、社員が応接室等に案内することとなっており、カウンター内に本社社員以外の者が入ることはできないようにしていた例**（大阪地裁平成 14 年 10 月 11 日）、**倉庫の鍵を、一般の従業者用のスペースとは区切られた取締役専用の部屋の鍵箱の中に保管していた例**（東京地裁平成 16 年 5 月 14 日）等がある。

一方、秘密管理性を認めなかったものとして、**顧客情報を記した台帳が施錠できる事務所内に置かれ、第三者が事務所内に侵入できないようになっていたが、事務所内では机の上に置かれていた例**（大阪地裁平成 16 年 5 月 20 日）、**製造している各種装置の図面が保管されている設計室の入口に、「厳守業者立入禁止」、「関係者以外立入禁止」及び「立入禁止工場内」とそれぞれ記載したボードが掲示されており、外注業者等の部外者は、原則として自由に出入りすることができないようになっていたが、原告従業者は、設計室に入ることについて特段制限されていなかった例**（大阪高裁平成 17 年 2 月 17 日）等がある。

【望ましい水準】

① 情報の区分と表示

秘密情報は、その他の情報と区分して管理することが必要である。秘密情報については、秘密性のレベルを決め、それに応じた管理を行うことが望ましい。

営業秘密であること及び秘密性の区分を、権限を持ってアクセスした者が客観的に認識可能な状態（マル秘マーク等）にすること、自社の営業秘密に他者の営業秘密が混入（コンタミネーション）しないようにすることが重要である。

（ア） 情報の秘密区分（秘密管理のレベル分け）

まず秘密情報をその他の情報と、区別することが必要である。その際、自社の情報については、情報の機密性のレベルに応じて区分することが望ましい。

通常、経営上極めて重要で、ごく限られた最小限の関係者のみに開示される情報は、「極秘」や「厳秘」等に分類されている。また、「極秘」ほど重要ではないが、限定された関係者のみにしか開示されない情報が「秘」に分類されることが多い。企業の中の情報全体からみると、「極秘」「厳秘」「秘」等に指定して厳しく管理する情報は、業種にもよるが、通常、それほど大きなウエイトを占めることは無いと考えられる。（あまりに多すぎれば、管理のコストが増大するとともに管理の実効性確保が困難になる。）

つまり、「極秘」や「厳秘」に区分される情報は、それ相当の厳格な管理が必要になることから、大多数の情報を「極秘」「厳秘」と設定すると、必要な情報の共有化が阻害される。また、「極秘」「厳秘」情報の相対的価値が低下する。

また、機密のレベルを区分する目的は、関係者の認識を共有化し、そのレベルに応じた管理を行うことにある。重要な営業秘密になるほど管理を厳格に行うことになるが、それを通じて全体として管理に過剰なコストをかけすぎないようにする点も重要である。

他社の情報については、当該他社の区分が付されていることが想定される。当該媒体を返還する義務がない場合や複製を許されている場合には、契約等の趣旨を踏まえつつ、自社の区分に基づき再区分を行い、かつ、それが他社情報であることがわかるようにしておくことが望ましい。

（イ） 客観的に認識可能な表示（営業秘密及び区分の表示）

営業秘密が「秘密として管理」されている情報であることを客観的に認識ができるようにするため、例えば、秘密情報が記載された部分の隅に秘密であることを示す明快・平易な言語・文字・デザイン・記号・マーク等を記載・記述することが考えられる。その際、それぞれの情報がどの機密性のレベルに属するものであるかが分かり、どのレベルで管理すればよいのかが分かるように、その秘密区分を表示するのが望ましい。

具体的な表示としては、紙媒体に記録されている情報であれば、「厳秘」や「秘」等のスタンプを押すことや、シールを貼付することなどが考えられる。電子情報

の場合は、フロッピーディスク等の記録媒体にシールを貼付することや、営業秘密であること及び、どの機密性のレベルかを表示するデータを電子情報そのものの中に組み込むこと、ファイルの開封に関する秘密レベルに応じたパスワードを設定する、あるいはファイルを暗号化することが考えられる。

②　アクセス権者の特定

誰がどの営業秘密にアクセスできるかをあらかじめ特定する。その際には、営業秘密へのアクセス記録を残すことにより、管理の実効性が増す。

誰がどの営業秘密にアクセスできるか、すなわち、「アクセス権者」をあらかじめ特定しておく必要がある)。固有名詞での特定でなくても、部門の長の許可を受けた部員のみが持ち出して使用できることとするといった方法も考えられる。

当該営業秘密を必要な人だけに開示をするということが重要であるという観点からは、機密性のレベルに応じてアクセス権者の範囲は異なり、機密レベルが高くなるほどアクセス権者の数は少なくなるべきものと考えられる。なお、こうした特定が行われていれば、アクセス権限のない者の情報入手は不正競争防止法第２条第１項第４号の不正取得に係る不正競争行為に該当することになる。

また、例えば、台帳のようなものを作成し、当該営業秘密を閲覧や複製した者を記録することも、アクセス権者以外の者によるアクセスを防ぐ上で有効である。

なお、アクセス権者以外の者が、アクセス権限に違反していないことを証明する手段として、「ペーパー・トレイル」（独自に制作した情報であることを立証するために、研究の軌跡等を記録する方法。以下同じ。）や、ソフトウェア開発におけるいわゆる「クリーン・ルーム」の手法（物理的にも場所を隔離することにより、他の営業秘密にアクセスしていない状態で開発していることを証明する方法。以下同じ。）等がある。

③　媒体の保管、持ち出し制限と廃棄

情報を媒体に記録した場合は、施錠可能な保管庫に、施錠して保管する必要がある。
また、持ち出し制限を行うとともに、媒体の廃棄の際には、焼却やシュレッダーによる処理、溶解、破壊等の措置を講ずることが重要である。

（ア）　保管

書類、ＣＤ－Ｒ又はメモリーカード等の情報を記録した媒体（ダウンロードして作成したものを含む。）は、アクセス権者以外の者がアクセスできない場所（例：部署内の特定の者が管理する施錠可能な保管庫（金庫、机の引き出し等））に施錠して保管する必要がある。

鍵にも簡易なものからセキュリティレベルの高いものまで様々あり、個々の秘密のレベルに応じて適切なものとすることが望ましい。

（イ）　持ち出し制限

アクセス権者による媒体の持ち出しを認める場合には、持出簿を作成し持出管理を行うこと、複写の制限、持出の期間や場所の制限（自宅への持ち帰りの禁止等）を行うことも考えられる。なお、アクセス権者による権限外の使用又は開示行為は、不正競争防止法第２条第１項第７号の不正競争行為に該当し得ることになる。

（ウ）　廃棄

情報が記録された媒体を廃棄する場合は、焼却、例えば、〇〇mm 以下となるシュレッダーによる処理、溶解、破壊等の復元不可能な措置を講ずることが重要である。

④　施設等の管理（建物・事務所・研究室等のセキュリティ配慮・警備）

営業秘密の保管場所の施錠や、保管されている施設への入退出を制限する。

秘密情報を保管する場所のセキュリティ配慮については、対象となる秘密情報の価値によってレベルの差があるものの、アクセス権者以外の者がアクセスできないよう管理されていることが必要となる。

具体的には、営業秘密の保管場所を施錠することや、「関係者以外立ち入り禁止」等の表示を設置すること、施設への入退を制限（ゾーニング）し、その入退出の記録を作成することが考えられる。また、警備員の夜間配置や警備システムの導入等様々な管理方法を活用し、セキュリティレベルを高めることが考えられる。例えば、ＩＣカードで本人確認した上で入館し、指紋や虹彩等の生体認証のチェックを受けて入室する場合等には、当該部屋の機密レベルが高いとみなされる可能性が高いと考えられる。

また、取引先から技術ノウハウの開示を受ける際、当該技術ノウハウと類似の自社技術を有し、それを用いて自社製品を開発しているような場合、他社技術と自社技術を扱う者を区別し、それぞれの部屋を分離して、それぞれの部屋には関係者以外は相互に入室できないようにする等、当該他社情報に自社の技術者・開発者がアクセスできないようにすることにより、コンタミネーション（情報の混入）を防ぐことが考えられる。

なお、①～④の全てについて、責任者を明確にした組織的管理が行われることが重要である（「５．組織的管理」を参照）。また、クリーン・ルームについては②を参照。

（３）技術的管理

コンピュータ機器類において管理されている情報は、必ずしも明確な記録媒体を特定できるわけではなく、インターネット等の発達により一度に大量の情報が世界中に伝達されるリスクをも考慮すれば、無体物である情報自体を管理することもますます重要になっている。

このような管理においては、情報の取扱いに関するマニュアルの設定、アクセス権者の限定、外部からの侵入に対する防御などが重要な要素となる。

【判例の動向】

まず、「マニュアルの設定」については、コンピュータやデータの取扱いに関して判示しているものがある。

秘密管理性を認めた例としては、**日々の業務が終了するごとに、システムに接続されたコンピュータの各端末の電源のみならず、サーバ･コンピュータ自体の電源を切ることとされていた例**（東京地裁平成 16 年 5 月 14 日）等がある。

一方、秘密管理性を認めなかった例として、**各種装置の図面の電子データを必要とする従業者が配布されたパソコンに当該図面を保存することを制限したことはなく、あるいは図面の電子データの取扱いに格別の指示をしたこともない例**（大阪高裁平成 17 年 2 月 17 日）等がある。

次に、「アクセス及びその管理者の限定」については、ユーザーID とパスワードを設定することについて判示されているものがある。

秘密管理性を認めた例としては、**バックアップ作業を行うに当たっては、特定のユーザー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例**（大阪地裁平成 15 年 2 月 27 日）、**顧客情報について、専用コンピュータ内にデータベース化して格納し、同社の全役員、従業者に対し、それぞれ個別のパスワード（毎月変更される。）を与え、右パスワードを使用しない限り本件顧客情報を取り出すことができず、第三者がこれを取り出す余地はないようにした例**（東京地裁平成 11 年 7 月 23 日）等がある。

一方、秘密管理性を認めなかった例として、**コンピュータを立ち上げるにはパスワードが必要であったが、付箋に記載されてコンピュータに貼ってあったため、従業者は、上記事務担当者以外の、商品発送に関わる者も含め、全員がパスワードを知っていた例**（東京地裁平成 15 年 5 月 15 日）、**原告の顧客データへのアクセスについてはパスワード等による保護はされておらず、事務所にいる者なら誰でもこのデータを見ることができる状態にあった例**（東京地裁平成 14 年 4 月 23 日）等がある。

その他、「外部からの侵入に対する防御」に関しては、営業秘密を管理するコンピュータと外部との接続状況について判示したものがある。

秘密管理性を認めたものとして自己の営業に関する情報を管理するコンピュータは**他のコンピュータ及びインターネットに接続されていない』例**（東京地裁平成 17 年 6 月 27 日）、**データベースが、会社外部と電気通信回線で接続されていないサーバ･コンピュータシステムに**

より作成、保管されていた例（東京地裁平成 16 年 5 月 14 日）等がある。

【望ましい水準】

事前に、電磁的に記録されている営業秘密の管理方法やデータ複製、バックアップを行う際等の各種ルールをマニュアル化あるいはシステム化しておくことが考えられる。

アクセス権者を特定すること、コンピュータやシステムを外部ネットワークから遮断すること、データを復元できないように破棄することなどが重要である。

① マニュアル等の設定

電磁的に記録されたデータを適切に管理する上では、基本的には（２）物理的管理と同様ではあるが、インターネット等のコンピュータ・ネットワークに接続する際のルールの確立、電子メール内容の暗号化、データ複製、バックアップをする際の手順の明確化やバックアップデータの暗号化等も考えられる。

② アクセス及びその管理者の特定

情報が電磁的記録で保管されている場合は、他の部署の者は閲覧することができないような技術的制約を加える等、機密性のレベルに応じた様々な管理が可能である。

また、当該コンピュータやファイルそのものの閲覧に関するパスワードの設定、パスワードの有効期限の設定や、同一又は類似パスワードの再利用の制限、アクセス記録のモニターなどにより技術的により高い秘密管理性を保つことが可能となる。

なお、ＩＤ、パスワード管理に関しては、情報セキュリティの管理者が退職した場合に最も注意が必要であり、その際には、管理者パスワードの確実な変更等を行うことも考えられる。

③ 外部からの侵入に対する防御

情報が電磁的記録で保管されている場合には、インターネットなどの外部ネットワークを通じて第三者が侵入し、営業秘密の盗み見などが行なわれることのないよう、営業秘密を扱っているコンピュータを、何らかの形で外部ネットワークから遮断しておくことが必要である。

例えば、営業秘密を管理しているコンピュータはインターネットに接続しない、ファイヤーウォール等で外部からの侵入を防止する。

ウイルス感染によるネットワークを通じた情報漏洩を防止するため、ウイルス対策ソフトウェアを導入するなど、対策に万全を期すことが重要である。

さらに、不注意による情報漏洩を防止するため、営業秘密を管理するコンピュータにファイル交換ソフトウェアや、不必要なソフトウェア等をインストールしない等の対策を講ずることも重要である。

④　データの消去、廃棄

電磁的記録化された秘密情報を使用・保管していたコンピュータ・サーバ等のコンピュータ機器類を廃棄する場合、又は他者に譲渡等する場合には、内蔵されている記憶装置（例：ハードディスク）内に残っている情報が誤って他者に開示されることのないよう、データの復元が出来ない方法による電磁的記録の消去又は物理的な破壊を実施することが重要である。

３． 人的管理[3]

（１）基本的な考え方

「２．物理的・技術的管理」におけるアクセス権者の特定により、管理の対象となる人は特定されるが、アクセス権者がそれを秘密として扱うことについての意識を持ち、実際に責務を果たすような状況になっていること、及びアクセス権者以外の者も、自社の秘密保護に関する認識を持ち、営業秘密侵害や漏洩を防止するような意識を持っていることが重要である。（注：法的な責務があっても、現実に秘密として管理されていると言えなければ、営業秘密性は認められない。（大阪地裁 平成 11 年 9 月 14 日）

アクセス権者については、企業としては誰がどのような秘密情報を扱っているかを把握した上で、誰にどのような義務を負わせるかを明確にする必要がある（この点については組織的に管理していることが重要である）。アクセス権者自身にとっても責務が明確であることは望ましいが、そうした責務に関して双方が納得できるような方法でその内容についての共通の認識が形成されることが望ましい。

そのためにも、アクセス権者以外の者も含めて、当該企業における営業秘密の取り扱いに関するルール等を明確に周知するために、日常的に教育・研修等を行っておくことが重要である。こうした状況を実現することによって、企業と従業者等が同じ方向性を持って協力しながら企業の営業秘密を守っていくことが可能になり、それが、最も実効性が高まる方法である。

また、特に営業秘密の漏洩に関して問題となりやすいのは退職者であるが、過去にアクセス権限があった者の場合においても、企業と退職者との間での退職後の責務に関する約束について、双方が納得感を得られていれば、同様に実効性の高い管理が実現できる。そうした約束においては、退職者としても、責務の範囲を明確化しておくことがその後の活動における自由度を高めることになるという点が重要である。

人の管理については、従業者等、退職者、派遣従業者、転入者、取引先等、対象に応じた適切な管理を行う必要がある。

[3] 「人的管理」とは、前掲 ISMS 認証基準 Ver.2.0 附属書「詳細管理策」では、「6. 人的セキュリティ」に相当するものである。

【判例の動向】

過去の裁判例では、「教育・研修の実施」や「就業規則・秘密保持契約」の存在について判示しているものがある。

まず、「教育・研修の実施」に関して秘密管理性を認めたものとして、**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徹底指導していた例**（東京地裁平成 12 年 11 月 13 日）、**従業者に対し、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**（東京地裁平成 16 年 5 月 14 日）、**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者に周知させていた例**（東京地裁平成 15 年 11 月 13 日）、**従業者に対し、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ていた例**（東京地裁平成 17 年 6 月 27 日）等がある。

次に、「就業規則・秘密保持契約」に関して秘密管理性を認めたものとして、就業規則に**社員は、会社が指示した秘密事項を自己の担当たると否とを問わず、一切外部に漏らしてはならず、秘密事項を発表しなければならないときは、原告の許可を受けなければならない旨の規定を設けていた例**（東京地裁　平成 11 年 7 月 23 日）、**営業秘密に接する機会のある従業者に対し、仕入先や顧客等の情報が営業秘密であって、これを原告の目的以外に使用しないこと等を記載した誓約書を提出させてきた例**（東京地裁平成 17 年 6 月 27 日）等がある。

一方、秘密管理性を認めなかったものとして、**就業規則にある「自己の所管の有無に関係なく会社の業務上の機密事項を他にもらさない。」との条項を規定しているが、業務上の機密事項に関する従業者の守秘義務を一般的に定めたものにすぎないとした例**（大阪高裁　平成 15 年 1 月 28 日）、**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者との間で厳格な秘密保持の約定を定めるなどの措置を執っていなかった例**（東京地裁　平成 16 年 4 月 13 日）、**就業規則に、「社員は、会社の機密、ノウハウ、出願予定の権利等に関する書類、テープ、ディスク等を会社の許可なく私的に使用し、複製し、会社施設外に持ち出し、または他に縦覧もしくは使用させてはならない。」、「社員は、第13条第3項に定めるところの他、業務上機密とされる事項および会社に不利益となる事項を他に漏らし、または漏らそうとしてはならない。社員でなくなった後においても同様とする。」という規定が置かれているが、当該規定はその対象となる秘密を具体的に定めない、同義反復的な内容にすぎないとした例**（東京地裁平成 17 年 2 月 25 日）、**就業規則中の規定は、書類等を厳重に保管すべき義務を従業者に課したものということができるが、同規定は、原告の備品等を大切にし、消耗品等を節約するというような規定と同列に規定されており、書類等の会社の備品等を取り扱う際の従業者の心構えを抽象的に定めた規定というべきであり、このような規定をもって営業情報が秘密として管理されていると客観的に認識し得るものではないとした例**（大阪地裁平成 17 年 5 月 24 日）等がある。

【望ましい水準】

（２）従業者に対する教育・研修の実施

秘密管理性を継続させるために、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教育を実施することが重要である。こうした教育の実施は、企業と従業者等との間での様々なレベルでの共感の醸成に資するほか、教育を受ける側にとっても責務の範囲が明確になるというメリットがある。教育の実施に当たっては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。

①　教育・研修責任者の設置

組織内における教育責任者を事前に定めておくことが考えられる。教育責任者は組織に属する者に対する定期的な教育に関する実施責任を有するものとし、このことを明らかにするため、秘密情報管理規程等に教育責任を固定化（例えば、セキュリティ管理責任者は教育責任を負う）することが考えられる。

教育責任者は、教育を定期的に実施する他、実際に講師を担当する者が秘密管理の概要を把握していることを確認することが必要である。

②　教育・研修内容の決定

組織形態や業種によっては実際に教育を行う者が必ずしも教育責任者であるとは限らない。したがって、教育内容を組織内で均一化するために事前に教育内容を定め、場合によって内容に差異が生じないよう配慮することが望ましいと考えられる。具体的には、教育ツールやカリキュラムの作成等、教育内容の事前設定等が考えられる。

なお、カリキュラムの一例としては、情報管理の重要性、秘密情報の管理組織、具体的な管理方法（○○株式会社　秘密情報管理規程の内容について）等が考えられる。

③　教育・研修の実施

営業秘密にアクセスする者に対して定期的な教育を実施することも望ましいと考えられる。具体的には階層別教育（例えば、新規採用者に対する教育、管理職に対する教育）等の既存の定期研修等の機会に組み込むことが合理的な実施方法の一つであると考えられる。

また、営業秘密の管理に関する一般的な教育・普及活動を行うほか、営業秘密を取り扱う頻度が高い従業者等に対しては、別途関連する法規制の内容、具体的な管理のあり方、事故が発生した場合の方法なども含めて教育、研修を実施することが重要である。

（３）従業者、退職者等に関する就業規則・契約等による秘密保持の要請

営業秘密の保護にあたっては、物理的･技術的管理や組織的管理に加え、契約により、営業秘密を開示した相手方に対して秘密保持義務を明確化することが重要である。

就業規則や各種規程に秘密保持義務を規定することは、在職中の役員･従業者に対する義務を明らかにする点で重要である。なお、就業規則に義務違反者に対する懲罰規定を設ける場合などには、特に労働関連法規を遵守する必要がある。

退職者に秘密保持義務を課す場合には、一般的には、秘密保持契約を締結する必要がある。

また、取引先に営業秘密を開示する場合にも、秘密保持義務を含んだ契約を締結する必要がある。

競業避止義務に関しては、直接的に「職業選択の自由」を制限するものであるので、秘密保持契約とは峻別することが望ましい。

①　就業規則等の規定

役員・従業者は、一般的には、それぞれ就任時の委任契約・就職の雇用契約に基づき、又はこれに付随する信義則上秘密保持義務を負うが、それを就業規則等に規定することが考えられる。

一方、就業規則において秘密保持の規定を設ける場合には、労働関連法規に反しないよう留意する必要がある。例えば、就業規則において、営業秘密を不正に取得及び使用又は開示した従業者に対する懲罰規定を新たに制定し、又はその内容を変更する場合には、労働基準法の規定に従い、使用者は労働組合又は労働者の過半数を代表する者の意見を聴き、その変更を労働基準監督署に届け出る必要がある（労働基準法第 89 条及び第 90 条）。また、作成された就業規則が民事的な効力を有するためには、事業場の労働者に対して周知されていること等も必要である。これらの際には、同法第 91 条（制裁規定の制限）の規定にも留意する必要がある。なお、これらの義務を就業規則等に規定する際には、秘密保持義務が必要性や合理性の点で公序良俗違反（民法第 90 条）とならないようにすべきである。

なお、企業が営業秘密管理規程を策定する際には、管理の実態を把握した上で、当該規程を確実に履行可能なものとなるよう、上記規程に係る従業者と協議するなどしてコンセンサスを形成することが望ましい。

ただし、就業規則等に基づく秘密保持義務は、包括的・一般的な義務規定に留まり、個々の従業者にとっては開示された情報のうち何が保護の対象となるか不明確な場合もある。このような場合には、就業規則等に、対象となる営業秘密の範囲は別途指定する旨規定し、個々の従業者毎に対象範囲を指定する方法が考えられる。

就業規則に規定された秘密保持義務の法的拘束力については、当該役員・従業者が退職したことをもって直ちに秘密保持義務が完全になくなるものではないと考えられるものの、より高いレベルでの保護が必要であれば、退職した元役員・従業者

との間で、秘密保持義務を課すという観点からは、後述のとおり、秘密保持契約等により、義務の存在を明確化することが必要となる。

② 従業者、退職者等と締結する契約

現職の役員・従業者に対しては、一般的には、それぞれ就任時の委任契約、就職時の雇用契約に基づき、又はこれに付随する信義則上、秘密保持義務を負う。

ただし、その内容等を明確にする観点から、個別の契約・誓約書等により秘密保持義務を課すことがある。

一方、退職者に対して秘密保持義務を課す場合には、一般的に秘密保持契約を締結する必要がある。特に、現職の従業者等及び退職者と秘密保持契約を締結する際には、秘密保持義務が必要性や合理性の点で公序良俗違反（民法第 90 条）とならないよう、その立場の違いに配慮しながら、両者がコンセンサスを形成できるようにすることが重要である。

③ 退職者との競業避止契約

秘密保持に関して、退職後の従業者等に対して競業避止義務を課すことも考えられる。しかしながら、競業避止義務の有効性の要件は、秘密保持義務よりも厳格に判断されている。秘密保持義務とは異なり、競業避止義務はより直接的に「職業選択の自由」を制限する恐れがあるので、秘密保持契約とは峻別することが望ましい。（競業避止義務の有無は、「秘密管理性」の判断とは別個のものである。）

なお、競業避止義務の有効性は、判例上、「債権者の利益（企業秘密の保護）、債務者の不利益（転職、再就職の不利益）及び社会的利害（独占集中のおそれ、それに伴う一般消費者の利害）の３つの視点に立って慎重に検討していくことを要する」とされ、「合理的範囲内」の競業制限でないとその有効性が認められない。かかる「合理的範囲」の具体的基準は、一般的に、①「制限の期間」、②「場所的範囲」、③「制限の対象となる職種の範囲」、④「代償の有無」等とされている。[4]（奈良地裁昭和 45 年 10 月 23 日）

また、退職後一定期間内に競業他社に就職した場合に、退職金の全部又は一部を減額する旨の規定を設け、違反があった場合に当該金額を支払わない／返還請求を行う運用も行われている。ただし、職業選択の自由等を不当に拘束するものは認められず、期間の限定等が必要である（具体的には、退職後の競業他社へ就職した場合において、退職金を一般の自己都合による退職時の退職金の半額とする旨の定めが有効とされた事件（最高裁昭和 52 年 8 月 9 日）や、退職後６ヶ月以内に競業他社に就職した場合は、退職金全額を支給しない旨の定めは、退職者に顕著な背信性がある場合に限り適用されるとした事件（名古屋高裁平成 2 年 8 月 31 日）がある）。

[4]具体的には、奈良地裁昭和 45 年 10 月 23 日判決は2年間、東京地裁平成 6 年 9 月 29 日判決は1年間の競業避止義務を有効としている。これに対し、浦和地裁平成 9 年 1 月 27 日決定は3年間、大阪地裁平成 10 年 12 月 22 日判決は5年間の競業避止義務を無効としている。

（４）派遣従業者

派遣従業者に対しても、同程度の業務に従事している自社の従業者に対して課しているのと同等の秘密保持義務を遵守するよう規定することが望ましいと考えられる。
ただし、これらの場合には、労働基準法や労働者派遣法に反しないよう留意する必要がある。

派遣従業者は、一般の従業者と同様に、派遣先（受入先の企業）の指揮命令を受けて派遣先の業務に従事する。しかしながら、派遣従業者は、あくまで派遣元（派遣会社）の従業者であり、派遣先と直接の雇用関係はない。派遣先の指揮命令権は、労働者派遣法に基づく派遣元・派遣先との間の派遣契約において規定されるものである。派遣従業者をどのような業務に従事させるかについては、派遣契約で明確化する義務があるが、営業秘密管理に関する秘密保持規定については、特段の義務は課されていないため、どの程度の秘密保持義務を課す必要があるのかを派遣契約等で明確化する必要がある。

その場合には、派遣従業者と同程度の業務に従事している自社の従業者に対して課しているのと同等の秘密保持義務を遵守するよう規定することが望ましいと考えられる。

ただし、これらの場合には、労働基準法や労働者派遣法に反しないよう留意する必要がある。派遣先企業と派遣従業者とが直接秘密保持契約を締結することが直ちに法律違反になるわけではないが、労働者派遣事業制度の趣旨からは、派遣先は、派遣従業者と直接秘密保持契約を締結するよりもむしろ、雇用主である派遣元事業主との間で秘密保持契約を締結し、派遣元事業主が派遣先に対し派遣従業者による秘密保持に関する責任を負うこととすることが望ましいものである。このほか、労働者派遣法によれば、派遣従業者は、その業務上取り扱ったことについて知り得た秘密を他に漏らしてはならない法律上の義務を負うものとされている。

このように、法的義務の点では従業者とは差異があるものの、営業秘密として表示を行い、アクセスを制限するといった、物理的・技術的管理の側面及び組織的管理の側面では、従業者と同様に妥当するものと解される。

※派遣先の秘密保持義務を派遣従業者に課す際に、派遣先が派遣従業者の個人情報を収集しようとする場合があるが、派遣先は、雇用主である派遣元事業主を通じて、派遣従業者の就業管理上の必要性が認められるものに限り派遣従業者の個人情報を収集することが基本であることに留意する必要がある。

（５）転入者

他の会社から転職した者を採用する時には、他者の情報に関するトラブルを回避する観点から、転職者が前職で負っていた秘密保持義務や競業避止義務の内容を確認することが必要である。

中途採用や第二新卒等により他の会社から転職して会社の従業者等になる場合、当該転入者が特定の情報に関し法的義務を負っていたことによりトラブルに巻き込まれることのないよう、コンタミネーション（情報の混入）に配慮することが必要である。

具体的には、その転入者が持ち込む情報によって、受入企業に差止請求による事業中断のリスクや何らかの損害賠償請求を受けるリスクが発生しないかどうかを検証することが必要である。

また、他社の営業秘密の取得及び使用又は開示を前提とした採用活動は行わないことは当然である。

①　転入者の契約関係の確認

採用予定者に対してインタビュー等をすることで、元の会社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が必要である。

具体的には、転入者の退職時の契約書等があれば、その秘密保持義務や競業避止義務の内容について確認しておく必要がある。その退職時の契約内容が対外的に確認可能であり、それが合理的であれば、安心して転入者を受け入れることができる。

ただし、採用予定者が退職時に差し入れた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契約を前職の会社との間で締結しているため、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、漏えいしてはならない、というような漠然とした契約の場合等には、明確な契約上の秘密保持義務の内容はわからない。この場合においても、少なくとも不正競争防止法上、転入者の秘密保持義務違反等につき「悪意」又は「重大なる過失」があれば法的責任が生じることから、「悪意・重過失」でないと評価されるように努めることが必要である。

例えば、従前の会社での業務内容・秘密保持義務の内容など、採用においてチェックすべきリストのようなものを策定しておくことも、コンタミネーション（情報の混入）を回避するための一つの方法として望ましい。また、従前の会社に対して、一定の合理的な質問状を送付することも考えられる。

最近では、従前の会社から警告書が届く場合もあるが、その場合には、その内容につき、当該転入者等に十分に確認することが重要である。

②　採用時の法的対処方法

コンタミネーション（情報の混入）を回避する法的方法としては、以下の点等が記載された誓約書を転入者から取得することが考えられる。このような誓約書の取得は、不正競争防止法上の「重大なる過失」が無いとの主張の一助となると考えられる。

- 他社の営業秘密を、その承諾なしに自社内に開示あるいは使用させないこと
- 他社において完成させた職務発明等の自社名義での出願をさせないこと
- 自社で就業するに当たり、不都合が生じる競業避止義務がないこと

もっとも、以上の方法も必ずしも完全にリスクを回避することはできるものではなく、不正競争行為に該当しないよう前述①のように自社で最善の注意義務を尽く

すことが望ましい。これら誓約書によってもなおリスクがあると考える場合には、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ことが望ましい。

③　採用後の管理

転入者の採用後も、当該転入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ことが望ましい。特に、転入者が前の企業に在職中に、自社の従業者と約束をして転入し、前の企業の営業秘密を開示した場合においては、法人処罰の対象となる可能性もあり、特に慎重な注意が必要である。また、配属についても、競業避止義務や秘密保持義務に十分に留意する必要がある。

（６）取引先

取引先の情報と自社情報の間で、コンタミネーションが生じないように管理を行うことが必要である。

①　自社情報

不正競争防止法の「営業秘密」として保護されるためには、取引先に開示する場合であっても、「秘密管理性」を維持することが必要となる。したがって、通常は、営業秘密の開示に先立ち、守秘義務を含んだ契約を締結することになる。この点、本契約書締結前であっても情報の開示が必要な場合もあり、例えば営業秘密に関するライセンス契約等の交渉当事者においては、相手方のノウハウの価値を評価させる目的で、本契約の交渉段階で、秘密保持契約を締結した上で当該ノウハウを開示する例がみられる。

さらに、会社間で取引を行う場合には、取引内容を明確化して無用なトラブルを防止するため、直裁的に、取引の開始時において秘密保持契約書を締結することが望ましい。ただし、契約上の守秘義務の範囲は、当事者で定めることから、不正競争防止法で保護される「営業秘密」に限られず、範囲が広範なことがある。開示された「すべての情報」が守秘義務の対象とされる場合も見受けられるが、情報を受領する側にとってはそれを遵守することが事実上困難な場合もあり、過度に広範であれば公序良俗違反（民法第９０条）として無効となる余地も考えられることから、どこまでが秘密保持の対象となるか明確に定めておくことが望ましい。

また、取引先に対しては、契約の中で、秘密保持義務のみならず必要に応じて取引先企業における営業秘密の適正管理について規定することも考えられる。ただし、それぞれの企業によって営業秘密の管理のレベルに差があることを考慮すべきである。相互に相手方の営業秘密を尊重し、管理する場合において情報の開示者の立場のみを考慮した契約にするのではなく、現実的に受入側の管理ができるよう、情報の性質と管理のレベルを契約書に具体的に規定する方が現実的な管理ができると考えられる。

② 取引先の情報

コンタミネーション（情報の混入）を防止するためには、以下のような対応が必要となる。

（ア） 契約締結時の留意事項

取引先からの営業秘密の取得に際しては、相手方の当該情報の開示につき正当な権限を有するか否か相当の注意を払う必要がある。例えば、重要なノウハウ等を開示してもらう場合には、事実上、相手方に当該ノウハウの帰属を確認するとともに、法律上、自社へのノウハウの開示が取引先の他の契約の債務不履行を構成しないこと等について、相手方取引先に表明又は保証してもらうこと等が考えられる。

（イ） 取引先への組織的対応

メーカー等においては、新規取引先から新技術・製品の売込みを受けることはしばしばあるが、企業規模が大きくなると、社内に担当窓口が複数存在する等、担当者レベルで個別に対応するときには統一的な管理が困難となることがある。このような場合は、技術・製品売込みに対する窓口を一本化して統一的な情報受領者管理を行うことが望ましいが、これが困難であれば、例えば統一的な取扱いルールを規定し、社内で対応を統一する方法も考えられる。

（ウ） 使用目的等による制限

他社から正当に取得した営業秘密であっても、「図利加害目的」で使用開示を行えば不正競争行為として損害賠償や差止めの対象となり、また、契約に基づき取得する場合は、当該契約で定めた範囲を超えれば契約違反となる。

このため、未然にトラブルを回避する観点からは、あらかじめ契約を締結し、取得する営業秘密の使用目的や開示先を明確に規定するとともに、使用又は開示の範囲について適正に管理を行うことが望ましい。なお、明示の契約がない場合であっても、信義則に反する使用又は開示は不正競争行為となることがあることに留意する必要がある。

４．　企業と従業者・退職者との適切な秘密保持契約の在り方

（１）秘密保持契約を締結する意義

企業が退職者と秘密保持契約を締結する意義は、契約法上の秘密保持義務を、企業が保護したいと考える営業秘密を保有した退職者に明確に負わせることである。

一方で、退職者もこの契約により義務の内容を明確にすることが出来る。

また、秘密管理性を判断する際に、個々の従業者との間で秘密保持契約を締結していたか否かを考慮に入れる裁判例が出ており、契約による義務を従業者に課すことが、秘密管理性を充足する際の１つの考慮要素となっている。

※なお、平成 17 年の不正競争防止法の改正に関する産業構造審議会知的財産政策部会不正競争防止小委員会における議論等の過程では、秘密保持契約に違反した場合も刑事罰の対象とすべきとの議論と、それへの慎重論があったが、対象となる秘密を明示した形での秘密保持契約の慣行が十分に根付いている状況にないこと等を理由に、平成１７年改正においては刑事罰の対象とすることは見送られた。

将来的に法規制の対象となるか否かは別として、従業者・退職者との間でより対象となる情報の範囲を明確にした秘密保持契約を締結することは極めて重要な意味を持つ。

（２）秘密保持契約の内容

秘密保持契約に盛り込む内容については、例えば①対象となる情報の範囲、②秘密保持義務及び付随義務、③例外規定、④秘密保持期間、⑤義務違反の際の措置等があげられる。

秘密保持契約に盛り込む内容については、例えば以下のような点が挙げられる。

①　対象となる情報の範囲

秘密保持契約では、義務を課す対象となる情報を特定することが必要となる。特定の程度は、どのような保護を受けるかによって異なるが、契約法上の観点からは、過度に広範な秘密保持契約は必要性・合理性の観点から公序良俗違反となり、保護を受けられなくなる可能性がある。

また、不正競争防止法上の営業秘密の要件の一つである「秘密管理性」の充足を否定した理由の一つとして、対象となる秘密を具体的に定めない、同義反復的な内容の就業規則の規定は、秘密管理性を充足するものにはならないことを挙げた裁判例（東京地裁平成 17 年 2 月 25 日[5]）がある。

---

[5] この判例は、就業規則中の、「（１３条３項）社員は、会社の機密、ノウハウ、出願予定の権利等に関する書類、テープ、ディスク等を会社の許可なく私的に使用し、複製し、会社施設外に持ち出し、または他に縦覧もしくは使用させてはならない。（１５条）社員は、第１３条第３項に定めるところの他、業務上機密とされる事項および会社に不利益となる事項を他に漏らし、または漏らそうとしてはならない。社員でなくなった後においても同様とする。」という規定に対す

対象となる情報について双方の理解が一致していなければ、それは、客観的認識可能性の問題となりえる。このため、秘密管理性の判断において対象の特定性が重要となってきている。

対象となる情報の特定は契約当事者双方の認識を共通化し、実効的な秘密管理を可能にすることになる。

具体的な特定方法として、下記の（ア）（イ）及び（ウ）が挙げられる。ただし、単に特定の程度が高いほど良いということではなく、双方の認識が一致する程度に特定されているか否かがポイントとなる。

したがって、特定の際には具体性が高いことが望ましいが、例えば契約書を通じた漏洩のリスクなどに配慮して具体化が難しい場合は、下記の（ア）、（イ）のような特定の仕方も有効である。いずれにしても契約の内容の開示を通じた秘密の漏洩の可能性については、契約の内容の開示に関する守秘義務を定める等の対応をとることが望ましい。

（ア）　メタ形式（概念）による特定

情報の内容に直接的に言及せずに、「～に関するデータ」「～についての手順」というように、情報カテゴリーを示すことにより、その外延を規定する方法である。

例えば、「新技術 A を利用して製造した試作品Ｂの強度に関する検査データ」、「B の製造における C 工程で使用される添加剤及び調合の手順」、「（他社である）D 社からの業務委託の際に提供を受けた５社以上からの借入を有する多重債務者のデータ」等の規定が考えられる。

（イ）　媒体による特定

営業秘密が記録された媒体の名称や番号等により、情報を特定する方法である。

例えば、「ラボノート X に記載された情報」「Y 社から提供されたファイル Z のうち○○ページに記載された情報」等の規定が考えられる。

これらの規定は、（ア）のメタ形式による特定と組み合わせることにより、「新技術Ａを利用して製造した試作品Ｂの強度に関するラボノートＸに記載された検査データ」のように特定性を高めることが可能である。

（ウ）　詳細な（クレーム類似の）特定

情報の内容そのものを記載する方法である。特に技術的情報の場合、特許のクレームに類似した形で規定する方法である。

例えば、「構成脂肪酸において炭素数○○以下の飽和脂肪酸含量が○○～○○重量％であり、炭素数○○以上の飽和脂肪酸含有量が○○～○○重量％である油脂配合物を、○○交換してなることを特徴とするクリーミング性改良油脂を、油相中に○○～○○重量％含有することを特徴とするバタークリーム。」等の規定が考えられる。

るものであるが、秘密保持契約についても同様の考え方が可能である。

② 秘密保持義務及び付随義務

基本的な義務として、営業秘密を目的外に使用すること、及び営業秘密を（アクセス権限のない）第三者に開示することを禁止すること（秘密保持義務）を規定する。

その他に、営業秘密を適正に管理するために、以下の点を規定することが重要である。

- 営業秘密が記録された媒体の複製・社外持ち出し・送信の禁止
- 営業秘密の適正な管理及び管理への協力
- 退職の際における営業秘密記録媒体（複製を含む。）の返還

③ 例外規定

契約において秘密保持義務の対象として、特定された範囲内に含まれる情報の中には、営業秘密に該当しないもの、あるいは営業秘密に該当するが入手方法等が不正競争防止法違反にならないものが含まれ得る。契約の有効性を高め、必要性・合理性がある範囲に限定するためには、こうした情報については、秘密保持義務の例外にすることが望ましい。

具体的には、

- 開示前から既に公知であった情報
- 開示後に受領者の責めに帰すべき事由なく公知となった情報
- 第三者から守秘義務を課されることなく取得した情報

などが挙げられる。

また、法律上の要求に基づき、行政機関や裁判所から当該営業秘密の開示を求められた等のやむを得ない場合も、秘密保持義務の例外として規定することも考えられる。この場合には、事前あるいは事後に開示者へ速やかに通知すること、秘密の開示を最小限度にすること（例として、民事訴訟の証拠として開示する場合に、インカメラ手続や秘密保持命令を活用する。）を義務付けることが考えられる。

④ 秘密保持期間

秘密保持義務の存続期間については、可能な限り期限を設定することが望ましいが、期限を設定することが困難である場合（法令上の理由、ライセンサーより無期限の秘密保持を設定されている等）も存在する。

秘密保持契約において、期限の設定が可能な場合はその期限を、困難である場合には（営業秘密性が失われるまで）無期限と明記し、秘密保持義務の存続期間とする。

なお、情報が公知となった際の無用なトラブルを避ける観点からは、当該営業秘密が秘密保持期間中に機密性を失った場合においては、元従業者からの問い合わせがあれば誠実に回答するなど認識を共有するための方策についての規定を設けるこ

とも考え得る。

⑤　義務違反に対する措置

営業秘密の不正取得及び不正取得された営業秘密の使用又は開示行為については、不正競争防止法上、差止請求権（第 3 条）、損害賠償請求権（第４条）、信用回復措置請求権（第７条）が規定されている。このため、契約において、その旨改めて規定せずとも、不正競争防止法上の権利は存在する。

一方、契約法上の観点からは、契約違反の場合における、損害賠償義務を規定することもある。また、弁護士費用等については、「損害」の中に含めることが困難な場合があるので、合理的な範囲内で求めることができるような規定を設けることも考えられる。

ただし、その場合には、労働基準法第 16 条に「使用者は、労働契約の不履行について違約金を定め、又は損害賠償額を予定する契約をしてはならない。」とあるため、違約金を定めたり、損害賠償額を予定することはできないことに留意する必要がある。

（３）秘密保持契約を締結するタイミングと事務手続き

秘密保持契約を締結するタイミングとしては、①入社時、②在職中（特定のプロジェクトへの参画時等）、③退社時があるが、①入社時の契約では、秘密保持義務の対象の特定は困難であるが、②在職中、③退社時には、具体的な特定が徐々に容易になることを踏まえ、双方の納得感が得られるような手続きを各企業が考え、タイミングに応じた秘密保持契約の進化を図る必要がある。

①　入社時

職種を限定して採用した従業者については、入社時に、その職務内容等に関連のある範囲内で秘密保持義務の対象となる情報を限定することが可能であると考えられるが、新卒や第二新卒採用等の場合、新入社員に対して今後どのような営業秘密が開示されるか予測することは困難である。

このため実務上は、包括的・一般的な秘密保持義務を規定した誓約書（又は契約）により、秘密保持義務を課す場合が一般的である。ただし、前述のとおり、退職後まで続く過度に広範な秘密保持義務を含む契約は、公序良俗違反となる可能性があること、何らかの形で事後的に範囲を限定することを検討する必要がある。

②　在職中（特定のプロジェクトへの参画時等）

企業にとって重要なプロジェクトに参画する場合や、特定の部署に異動し、新たな営業秘密を知ることとなった場合に、その都度秘密保持契約を締結することがある。

この場合、プロジェクトに関係する範囲、あるいは新しい部署の業務に関係する

範囲で、秘密保持義務の対象を限定することは可能である。

また、プロジェクトの終了後においては、さらに秘密保持義務の対象となる情報を特定することが容易になるので、終了後に契約を締結する、あるいは参画時に締結した契約に基づき、対象となる情報の範囲を終了時に確認するといった方法もあり得る。

こうした在職中の契約は、入社時の契約と比較して、対象となる秘密が特定されるとともに、契約を締結する人も限定的であるため、必要性・合理性の観点からも契約の有効性は高まると考えられるとともに、退職時までの期間がより短くなっていることから、当該従業者が秘密保持義務を負っているという認識も、より高いものになる。

③　退職時

退職時においては、今後どのような営業秘密にアクセスするか予想することが困難である入社時や在職時に比べ、各種プロジェクト等、実際にアクセスした営業秘密について確認的に特定を行うものであることから、秘密保持義務の対象となる情報を特定することは容易であるため、具体的な秘密保持義務の範囲を明示して契約を締結することが可能である。

しかし、この時点で突然契約の話をされると、退職者は当惑する可能性がある。それまでに契約を締結していない場合には、退職時に秘密保持契約を締結する可能性があることを事前に周知しておくこと、退職時までに何らかの契約を締結している場合には、守秘義務の対象となる情報の特定のみを退職時に行うこととするといった方策や、一定期間毎に契約の内容を見直すこともあり得る。

※個人情報保護法の施行に伴う留意点

平成 17 年 4 月の個人情報保護法の施行を期に、個人情報保護を名目として、個人情報とは無関係の営業秘密をも対象とする包括的な秘密保持契約を締結する場合がある。

しかしながら、個人情報保護と営業秘密の保護はその目的・範囲等が異なるため、従業者側の「納得感」の向上の観点からは、個人情報保護に関する契約と営業秘密に関する秘密保持契約は峻別する（別書面であるか否かは問わない）ことが望ましい。

（４）企業間の秘密保持契約との関係

①　企業間の秘密保持契約の特徴

企業間の秘密保持契約においても、基本的に企業と従業者等・退職者との間の秘密保持契約と同様の内容が規定されると考えられるが、企業間の秘密保持契約に特有と考えられる事項としては、以下の点が挙げられる。

（ア）　対象となる情報の範囲の変更

一般的には、事前に秘密保持契約を締結した上で、企業間で営業秘密を開示することになるが、事前に実際に開示される全ての営業秘密の内容を特定することは容易ではない場合がある。例えば、共同開発等の過程で当初の想定を超えるものについて口頭で開示した情報の中に、営業秘密が含まれる場合もある。

このような情報に秘密保持義務を課す場合には、あらかじめ口頭で開示した情報の取扱いに関する規定を別途設ける必要がある。具体的には、口頭で開示した情報については、開示した側が、情報の開示後一定期間内に当該情報の内容を文書化し、当該文書を秘密保持義務の対象とすること等が考えられる。

また、契約の存否自体が営業秘密に該当し、秘密保持義務の対象となる場合も考えられる。

（イ）　秘密管理体制の構築の要請

当該営業秘密の秘密管理性及び非公知性を維持するために、営業秘密の開示を受ける側に対して、秘密を適正に保護する体制の構築を求めることがある。

その一環として、当該営業秘密を実際に扱うこととなる従業者を特定し、その者に対して契約等により退職後においても秘密保持義務が課されるように措置することを求めること等が挙げられる。

（ウ）　契約期間と秘密保持義務の存続期間

企業間の秘密保持契約では、契約期間よりも秘密保持義務の存続期間を長く設定することがある。

これは、契約期間は、契約に規定された目的を達成するのに必要な期間であり、全ての規定の遵守を求めるものであるのに対し、秘密保持義務の存続期間は、契約条項の中でも、秘密保持義務についてのみ、より長期の存続を求める場合があるからである。

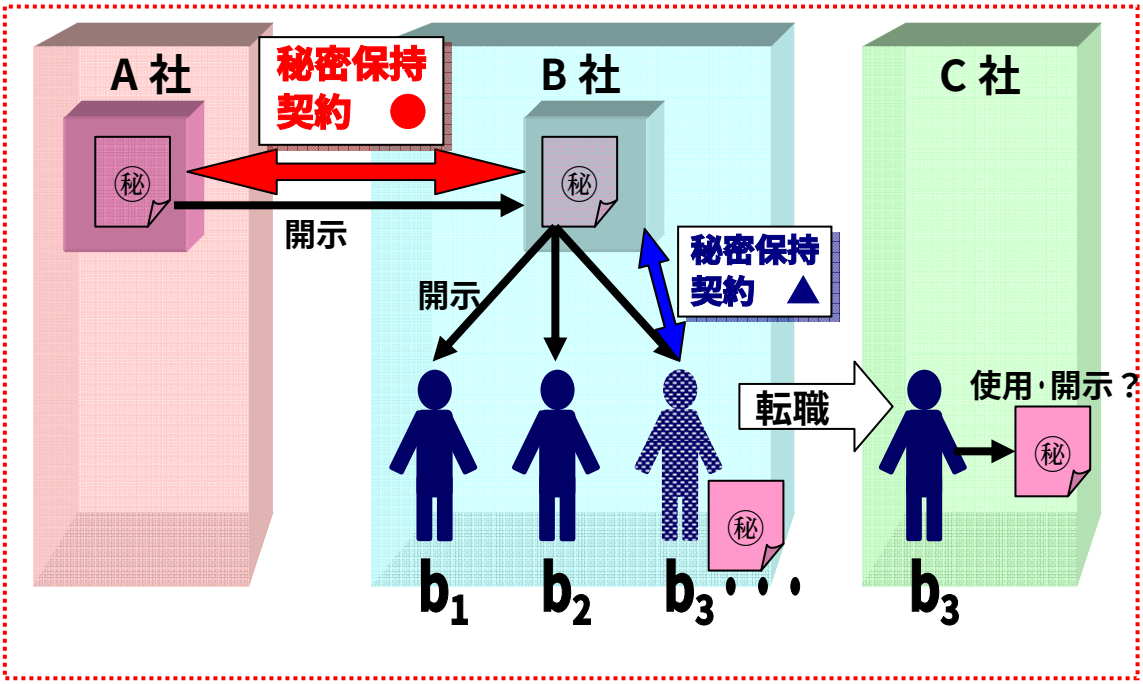
② 企業間の秘密保持契約と、企業と従業者等・退職者との間の契約の関係

企業が従業者等・退職者との関係で締結する秘密保持契約は、企業間で締結された秘密保持契約と密接に関係する場合がある。

例えば、ライセンス契約を結んで A 社（ライセンサー）の営業秘密を B 社（ライセンシー）に開示する場合、両社は秘密保持契約●を締結し、それに基づきA社は B 社に対して秘密管理体制の構築を要請する。

この場合において、B 社では、実際に開示を受けた営業秘密を使用するのは、B 社の従業者 b_1、b_2、b_3…であるが、B 社が b_3 との間で秘密保持契約▲を締結していない場合、B社従業者の一人である b_3 が C 社に転職した場合に、b_3 による A 社の営業秘密の使用又は開示を差止めることができなくなる可能性がある。

この場合、b_3 のみならず、B 社についても適切な秘密管理体制を構築しなかったとして損害賠償の責を負う場合があり得る。



言い換えれば、企業間で締結された秘密保持契約●は、開示先企業が、実際に営業秘密を使用する自社の従業者との間で秘密保持契約▲を締結しなければ、実効性が担保できない場合があり得る。実効性を担保するためには、両方の契約（●及び▲）の間に整合性がとれていることが必要である。

５． 組織的管理[6]

営業秘密の管理においては、個別の物理的・技術的・人的管理措置を実効的に実施し、問題が発生した場合に的確に対応していくための組織的な管理を行うことが必要である。

その際、①自社の営業秘密（他社から正当に開示を受けたものを含む。）を、外部に漏洩させないこと、②自社の従業者等が、他社の営業秘密を、不正に取得し、不正取得した営業秘密を使用又は開示しないことという両面からのアプローチが必要になる。

以下、（１）（２）でそれぞれ一般的に講ずるべき措置について述べ、（３）では、組織的な管理に関する望ましい水準について記載する。

（１）自社の営業秘密の管理のための組織的管理

自社の営業秘密を適切に管理するためには、その情報を物理的・技術的に管理し、それにアクセスする者について人的管理を行うことに加え、システムとして組織的に管理を行うことが重要である。

これは、自社の営業秘密の漏洩を防ぎ、漏洩あるいはその危険性を早期に発見し、状況を改善していくことを目的とするものであり、この仕組みを適切に機能させるためには、従業者等の責任と権限を明確に定め、営業秘密管理に関する規程や手順を整備し、その実施状況を確認して、それらの見直し及び改善、事故又は違反への対処などを継続的に行う必要がある。

前述の物理的・技術的管理及び人的管理が、このような組織としての対応のシステムの中に組み込まれれば、その実効性もより高まるものと考えられる。

【判例の動向】

組織的管理について判示している裁判例はあまり多くない。

その中では、秘密管理性を認めた例としては、**印字された顧客名簿を外部へ持ち出す場合には、顧客名簿社外持出許可書の用紙に必要事項を記入し、社長の決裁を受けることとして』おり**、かつ『**印字された顧客名簿については、使用後シュレッダー等で処分することを原則とするが、保存する場合には、施錠されている保管室に保管し、七年経過後に、原告従業者立会いの下に、専門業者に焼却を依頼するようにしている例**（東京地裁平成 11 年 7 月 23 日）、**派遣社員の名簿が営業秘密である事例において、外部から派遣社員あてに電話がかかってきたような際も、直ちに派遣社員の派遣先を教えることはせず、いったん電話を切り、改めて確認の上、派遣社員自身から連絡するように周知徹底させていた例**（大阪高裁平成 14 年 10 月 11 日）等がある。

一方、秘密管理性を認めなかった例として、**顧客データをコピーすることも禁じられておらず、かえって顧客データを使用する場合はコピーしてから行うこととされていた例**（東京地裁平成 14 年 4 月 23 日）、**電話での問い合わせにも特に制限なく会員情報が伝えられ、これらの者との間に秘密保持契約も締結されていなかった例**（東京地裁平成 15 年 5 月 15 日）等がある。

---

6 「組織的管理」とは、前掲 ISMS 認証基準 Ver.2.0 附属書「詳細管理策」では、「4. 組織のセキュリティ」に相当するものである。

（２）他社の営業秘密を侵害しないための組織的管理

平成 17 年の不正競争防止法改正により、法人の代表者や従業者等が、正当に示されていない他社の営業秘密を不正に取得した上で、使用又は開示した場合には、当該行為者に加え、法人も処罰されることとなった。

一方で、営業秘密が正当に示されたか否かにかかわらず、従業者が営業秘密の不正取得及び不正取得した営業秘密の使用又は開示を行った場合には、その従業者が所属している法人が、行為者と連帯して不正競争防止法上の民事的責任を問われることになり得る。さらに、企業が他社の営業秘密の侵害にかかわった場合には、社会的な責任という観点からその企業の評判に大きな影響を与える可能性もある。

したがって、企業としては、最低限両罰規定による刑事的制裁を回避し、さらにビジネス上生じるリスクをいかに回避するか、という観点から、自社の従業者等による営業秘密侵害行為への加担を未然に防止するための、積極的・具体的な措置を講ずることが望ましい。

①　両罰規定と選任監督義務（刑事的措置）

法人処罰については、第２章で述べたように、営業秘密侵害罪の行為者とともに、行為者が属する法人等が処罰の対象となる。

両罰規定に関する過去の最高裁判例では、法人の行為者たる従業者等の選任・監督その他違反行為を防止するために必要な『注意を尽したことの証明がなされない限り、事業主もまた刑責を免れ得ないとする法意』であることを判示している（最高裁昭和 40 年 3 月 26 日）。すなわち、法人には過失が推定され、注意を尽くしたことが証明されない限り、事業主は刑事責任を免れない。

また、『事業主が違反の防止に必要な措置をするとは、当該違反防止のため客観的に必要と認められる措置をすることであり、従って、それは、事業主が、単に一般的、抽象的に違反防止の注意、警告をしただけで足りるものではなく、違反行為の発生を有効に防止するに足りる相当にして具体的な措置を実施することを要すると解すべきである。』（高松高裁昭和 46 年 11 月 9 日）という高裁判例もあり、営業秘密侵害罪についても、基本的にはこれらの判決と同様の考え方に立って具体的な措置を講ずる必要がある。

②　相当の注意（民事的措置）

他社の営業秘密の取得に際して、営業秘密の不正取得行為（同法第２条第１項第４号）や不正開示行為（同項第７号）が介在することについて「悪意」又は「重大な過失」で取得等をした場合には、「不正競争」行為（同項第５号及び第８号）に該当する。

言い換えれば、従業者等が営業秘密の不正取得・開示行為等を行い、その者を通じて、企業が悪意又は重過失で営業秘密を取得した場合には、企業自身による「不正競争」行為に該当し、損害賠償等の責を負うことになり得る。

したがって、従業者が正当に営業秘密を取得・開示していることにつき、企業としては相当の注意を払う必要がある。

③　目安となる事項

企業が組織的な取組みを行うにあたっては、当該企業にとって「自社の何が重要であるか」が明確であることが基本となる。自社にとって重要な情報が組織的に管理されており、かつ、その創出経緯が明確になっていれば、新たに自社にとって重要な情報が入ってきた時に、それが自社のものか否かすぐに判別できる。一方、自社の情報でない場合には、その出所を明確にすることによって、他社の営業秘密の侵害行為に当たるか否かが判断可能となる。出所の表示に対しては、ほとんどの従業者が注意を払うはずであり、またそのようになっていれば、従業者等によるこうした侵害行為も抑止される効果があると考えられる。

こうした取組を前提とした上で、さらに実効的な管理体制を敷く必要がある。その際の目安となる事項として、以下の６項目が挙げられる。

＜目安となる６項目＞

（ア）　管理方針等（基本方針、基準、規程等）の整備

営業秘密管理上の不正を未然に防ぐための管理方針等（基本方針、基準、規程等）を整備し、またそれを具体化するための手続きが確立されていることが重要である。

ただし、これは、他の内部統制活動と分離された独立の文書類や手続きである必要はない。また、これらは監査の結果を踏まえて、継続的に見直しを行うことが重要である。

（イ）　責任者の存在とその権限の明確化

上記の管理方針等が正しく守られているかどうかを監督する責任者がいること、またその責任者の存在が組織内で周知されていることが重要である。

子会社・関連会社について、何らかの理由で、各社内での監督が十分に機能しない場合には、親会社の責任者はこれを放置することなく、当該子会社・関連会社と協議して必要な対策を講じ、必要に応じて、親会社として合理的な支援を行うことが考えられる。

（ウ）　営業秘密侵害を防止するための教育及び管理方針等の周知・徹底

営業秘密管理に関する教育や研修への参加を義務づけることで、あるいはどのように行動すべきかを説明した文書等を配布することで、上記管理方針等、手続きを従業者に周知徹底することが重要である。

ただし、教育・研修は、全従業者を対象にした画一的な教育よりも、むしろ、職場や職務ごとのリスクに応じたものとすることが望まれる。

また、企業側から見た営業秘密保護の観点だけでなく、従業者保護の観点から、従業者が営業秘密侵害罪に問われないよう、予防立証を含む自衛手段等についても、教育・研修をすることが望ましいと考えられる。

（エ）　日常的なモニタリングの実施

法令に抵触するか否かを事前に相談できる体制（例えば相談窓口の設置等）を社内に整備することが重要である。

日常的な情報収集活動が営業秘密の不正取得と誤解される可能性がある場合も考えられるため、例えば当該行為が法令に抵触するか否かを相談できる窓口等を社内に整備することが考えられる。また、相談例を蓄積し、管理方針等の見直しや、従業者への教育・普及活動に活用することが望ましい。

また、日常的な業務活動の中で、各レベルの責任者が、不自然な技術開発の進展や顧客の増大等、特に営業秘密の不正取得が疑われるような端緒があった場合には、組織として情報の出所を確認することが望ましい。

（オ）　内部監査の実施

営業秘密侵害のリスクに応じた内部監査を実施することが重要である。

リスクに応じた監査とは、一般的に言えば、仕事の性質上、営業秘密侵害が発生しそうな職場に対しては、包括的かつ高い頻度で、また逆にそうではない職場に対しては、限定的かつ低い頻度で、監査を実施することを指す。ただし、これは、他の内部統制活動と分離された独立の活動として展開する必要はない。

なお、一般に、内部監査のみでは、すべての問題行為を発見できるとは限らないため、例えば内部者からの報告等により潜在的な問題が発見された場合、その経験を踏まえて、監査項目や監査対象等を見直し、監査の精度を継続的に改善することが重要である。

（カ）　事後対応体制の整備

営業秘密管理に関する一貫した懲戒処分基準をあらかじめ設け、その内容を従業者に周知することが重要である。

その中には、不正を指示した者、また上司の指示などにより不正に関与しながらも、自らの過ちを報告してきた者などに対する措置、さらには不正を知りながら報告しなかった者の扱いなども含むことが重要である。

上記６つの項目は、免責のための必要十分条件ではない。つまり、これらを満たせば直ちに法人が免責されるというものではなく、反対に、これらの項目を一つでも満たさなければ、直ちに法人処罰が科されるというものでもない。「違反行為の発生を有効に防止するに足りる相当にして具体的な措置」といえるような実効的手段が執られていた場合には、それをもって法人が免責されることもあり得る。

なお、取り組みにあたっては、従業者全ての行動や社内の情報の全てを管理しようとしても、コストが増大するとともに実効的な管理が難しくなる。このため、それぞれの情報の重要性や従業者の任務の性質、コンタミネーション（情報の混入）が生じる可能性の高い場面等を分類することが重要である。その上で、営業秘密の侵害が発生するリスクやリスクが顕在化した場合のダメージ、管理を行う上でのコスト等を勘案し、「（３）　望ましい管理方法」で挙げる具体的な管理方法を参考に

しながら、個々の企業の経営判断によって必要な措置を講ずることが求められる。

（３）望ましい管理方法

自社の営業秘密を適切に管理するための組織的管理と、他社の営業秘密を侵害しないための組織的な管理の二つの側面から、適切に管理を行う。

その際、管理方針等の策定（Plan）、実施（Do）、管理状況の監査（Check）、見直し（Act）という、マネジメントサイクル（ＰＤＣＡサイクル）を確立することが重要である。

なお、企業が、上述の取組みを行うに際しては、国内法令を遵守することが当然の前提であるが、企業活動がグローバル化していることを考慮すると、企業のリスクマネジメントの観点からは、外国からの技術情報の導入に際して、例えば経済スパイ防止法等の当該国における法規制との関係にも配慮することが望ましい。

①　管理方針等（基本方針、基準、規程等）の策定＜Plan＞

基本方針を文書化して定め、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が望ましい。

（ア）　基本方針の策定

営業秘密管理の基本方針（ポリシー）は、営業秘密の管理に関する組織の意思を明示する大変重要なものであり、その組織の経営に関する基本方針の一部分であって、簡潔かつ理解しやすい形で文書化し、すべての従業者等に周知することが重要である。

また、組織の最高責任者がこれを制定・公表するとともに、Plan-Do-Check-Act のマネジメント・サイクル（PDCA サイクル）の中で、定期的に見直しを行い、継続的に改善することが望ましい。

具体的な基本方針の策定にあたっては、自社の営業秘密管理、他社の営業秘密侵害を防止する観点から、以下の事項を含むことが望ましいと考えられる。

- 営業秘密管理への取組の宣言
- 目的
- 対象範囲
- 用語の定義
- 基本原則
- 法令の遵守
- 罰則等

また、他社の営業秘密侵害を防止する観点からは、特に具体的に、以下の内容を盛り込むとさらに望ましいと考えられる。

＜具体的対応例＞

【情報取得の適正化】
・侵入や不正な利益の提供等、不正な手段での情報入手の禁止
・情報の出所の明示
・責任者、上司等による情報の入手経路の明確化

【情報管理の適正化】
（特に他社情報を預かった場合、他社から中途採用を行った場合）
・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（営業秘密性の明示及びアクセス制限）
・他社情報と自社情報の明確な分離とコンタミネーションの防止
・他社営業秘密に関する中途採用者の責任

【侵害が発覚した場合の措置】
・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
・侵害を行った従業者に対する懲戒・刑事告発等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、問題事実の公表

（イ）　実施計画の策定

基本方針のみでは、具体的な営業秘密管理の手順が必ずしも明らかではないため、具体的な営業秘密管理の目的と目標とを定めて、これを達成するための実施計画（プログラム）を策定し実行することが考えられる。

実施計画の策定にあたっては、まず営業秘密管理に関するリスクを洗い出した上で、リスクが顕在化した際に会社に与える影響の大きさ、またリスクが実際の問題にまで発展する可能性の大小、といった観点から、リスクに優先順位をつけ、優先順位の高いリスクをコントロールするための実施計画を策定することが望ましい。なお、会社の経営資源には限りがあるため、実施計画は、重要かつ緊急の課題への対応に絞りながら、しかも長期的にはリスク全体を軽減していくものとして策定することが考えられる。

その上で、管理目的は可能な限り明確に定め、管理目標は、可能であれば、客観的に把握できるような数値を用いて定める。また、基本方針等との整合性が保たれていることが重要であり、具体的な実施計画には次の事項を含めることが望ましいと考えられる。

- 目的及び目標を達成するための責任の所在の明示
- 目的及び目標を達成するための手段とスケジュール

（ウ）　ルールの構築（社内における開示・公表ルール）

上記の基本方針、実施計画のほか、営業秘密に関する各種規程（社内における開示・公表ルール、秘密性の区分とそれに応じた管理に関するルール等）などの社内ルールを設け、従業者等に周知徹底を図るとともに、具体的な営業秘密の取

扱い方法等を明示することが重要である。

具体的には、以下のような例が考えられる。

- 社外に秘密情報を開示する際には（相手方に秘密保持義務を課す場合でも）その開示の可否に付き事前にチェックを行い、社内手続きにおいて開示判断の権限を与えられた適切な者を承認に係らせることにより、不必要な開示を防止する（社内稟議システム等）。
- マスコミや学術誌への発表あるいは取材対応に関する公表ルールを作成する（情報管理規程作成）。（インサイダー取引規制関係等の公表ルールがある場合には、これらとの調整が必要となる。）
- 社内のある部門が開示又は公表した情報が、他の部門が開示又は公表を控えていた秘密情報であった、という事態の発生を防ぐため、情報を一元的に管理する（対外的な発表は広報室を通して行う等）。（広報・ＩＲ組織の設置・活用。）
- 営業秘密を開示した従業者等が退職する際には、その者が退職時に占有している会社の営業秘密に関する書類等を、その複製物も含めて返還させる。（返還ルールの明確化）

（エ）　各種規程類の文書化

上記、ア）～ウ）の管理方針等については、すべて文書化して、これを保存・管理することが必要である。

文書化の程度は、組織の規模、活動内容、ビジネス・プロセス及びその相互関係の複雑さ、関係する要員の力量等によって異なるものと考えられる。

具体的な姿としては、営業秘密だけでなく、個人情報等すべての情報を対象にマネジメント・システムを構築する場合においては、情報セキュリティ・ポリシーの一部分を構成する形で文書化する場合も考えられる。

② 実施（責任者の設置、従業者への周知徹底）＜do＞

組織体制を整備し、それぞれの責務を明確にして管理方針等を実施する。そのために、従業者等がどのように行動すべきか等について、社内において周知を徹底する。
また、各組織のレベルに合わせた責任体制を構築して運用する。

（ア） 責任者の存在とその権限の明確化

上記の管理方針等に則り、具体的な物理的・人的管理を行うための管理責任者がいること、またその責任者の存在が組織内で周知されていることが重要である。

子会社・関連会社について、何らかの理由で、各社内での監督が十分に機能しない場合には、親会社の責任者がこれを放置することなく、当該子会社・関連会社と協議して必要な対策を講じ、必要に応じて、親会社として合理的な支援を行うことが考えられる。

＜具体的対応例＞

○営業秘密を含む自社・他社情報の取扱責任者を設定する。
○段階毎に（会社（関連企業を含む）全体、事業所単位、部課単位、プロジェクト単位等）責任者の設定、及び報告体制を整備する。
○これらの組織体制を整備するにあたっては、法務部や知財部等の一部部署だけではなく、事業活動に関わるあらゆる部署を関与させて実施することが必要となる。

a) 総括責任･統括責任

責任の体系によって、以下の二つに分類する。

○統括責任

会社全体の情報セキュリティ管理の統括責任である。役員の中から、情報セキュリティを担当する役員を指名し、この責任を担わせるのが適切である。このような役員を CISO（Chief Information Security Officer、情報セキュリティ担当役員）と呼び、「c)望ましい組織体制の例」で述べる情報セキュリティ委員会の委員長の役割を担わせる。

○総括責任

担当事業所において、情報セキュリティ管理に関する全社的な管理方針等が正しく運用されていることを確認する責任である。通常、営業所長、工場長等、

事業所長が、これを担う。

b)　情報セキュリティ管理責任

情報セキュリティの管理責任は、その性格から次の２つに区分される。企業の規模等によっては、個人情報保護責任者や情報セキュリティ責任者等と兼務することもあり得る。

○情報管理責任

情報管理責任は、次のような事項から構成され、当該情報を作成した者の所属する組織の責任者が行うのが適切である。ただし、以下の推定、特定等について、組織全体として統一的な把握・管理が統括責任の下で行われることが必要である。

- 「厳秘」、「秘」等の秘密区分の指定
- 秘密区分の期限の明示
- アクセス権者の特定
- 社外への持ち出し及び他者への開示に係る許可等の判断
- 使用目的の設定

○セキュリティ管理責任

セキュリティの３要素、すなわち、機密性、完全性（保全性）、可用性のすべてを確保する責任である。言い換えれば、営業秘密について、正式に許可された者だけが、正しい内容の情報を、必要なときにはいつでも利用できる状態に管理する責任である。セキュリティ管理責任は、経営資源の一部分として、すべての組織責任者が担うべき性格のものである。

c)　望ましい組織体制の例

a)、b)のような責任体系に基づいて管理方針等を実施していくための組織体制について、その望ましい姿の例を示す。

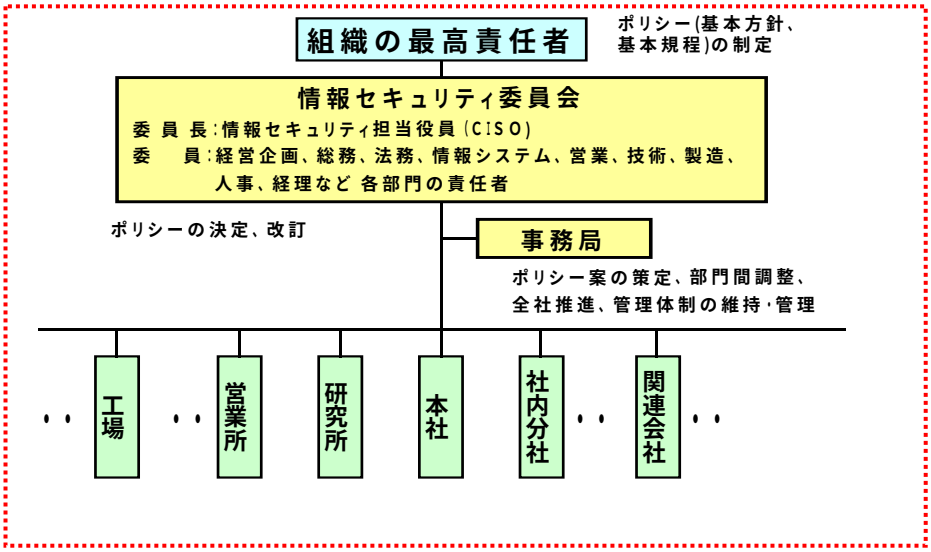
次図は、情報セキュリティ管理体制の例を示した図である。営業秘密を含む情報セキュリティ管理の基本方針や基本規程の制定及び改定は、組織の最高責任者が行うのが望ましいと考えられる。

また、組織の最高責任者のもとに、基本方針の決定、改定等に関する意思決定を行う「情報セキュリティ委員会」を設置することが望まれる。委員長は CISO が務め、委員には経営企画、総務、法務、情報システム、営業、技術、製造、人事、経理等社内各部門の責任者を充てる。

委員会は、基本方針案の策定、全社推進、部門間の調整、管理体制の維持・

管理等の機能を担う事務局を置く。事務局には社内に存在する営業秘密について広く現状を把握し、その取扱いを検討するのに十分な識見を有するメンバーで構成するのが望ましい。事務局を２つに分割して、情報セキュリティ委員会の事務を司る機能と専門的識見に基づいて基本方針案等を策定したり見直したりする機能とに分けることも有効である。

このような本社機構における組織体制の下に、社内全事業所をその傘下に置いて、全社的に統一された体制をとるのが望ましい。



（イ）　責務の着実な実施

２．～４．の物理的・技術的な管理及び人的管理を、それぞれの任にある者が着実に実施し、（ア）責任者がそれぞれのレベルで、その状況を管理する。その際は、それぞれの実施に関する記録を残すことが望ましい。こうした実施を確実なものとするために、（ウ）の教育を行う。

また、他社の情報については、当該従業者の日常的な情報収集活動など自らの行為が法令に抵触するか否かを事前に相談できるような体制（例えば相談窓口の設置等）を社内に整備することが有用である。

さらに、日常的な業務活動の中で、各レベルの責任者が、不自然な技術開発の進展や顧客の増大等、特に営業秘密の不正取得が疑われるような端緒があった場合に、情報の出所を確認することが望ましく、具体的には、以下のような対応が考えられる。

＜具体的対応例＞

○情報取得行為が不正競争防止法等に違反していないかを相談できる窓口を設置する。
○相談窓口等に寄せられた内容や、過去に発生した問題行動を具体的に分析して、必要に応じて管理方針等の改訂を行う。
○特に営業秘密に接する可能性の高い事例において、営業秘密侵害が発生するリスクとその対処方法を検討し、他社の営業秘密に接する可能性の高い従業者に対してモニタリングを行う。
○営業秘密の不正取得が疑われるような端緒を発見した場合に、情報の出所等について、現場部門の責任者等がモニタリングを実施する。
（例）
・今まで検討したことのないような技術情報が記録された媒体等を発見した場合
・新規顧客が急速に拡大した場合
・情報に対して高額の対価を支出する場合

特に、他社の営業秘密を取得する可能性が高いケースと、それに対する対応として、以下のものが挙げられる。

（ケース毎の例）

●共同開発時
・共同開発にあたり、他社から営業秘密の提供を受ける場合には、（特に媒体でない場合には）先方と協議の上、可能な限り営業秘密の特定を行い、意図せずして、他社の営業秘密の不正使用又は開示を行うことがないよう配慮する。
・口頭で情報の提供を受けた場合には、事後に文書等で営業秘密に該当する情報の確認を行うことで、トラブルを未然に回避する。
・研究機関、大学等と研究を行う場合、競合他社等も並行して研究を行っている場合があるため、先方に対する確認を行なうとともに、企業の担当者に対する事前の教育等を徹底するとともに、必要に応じ、秘密保持契約等の措置を講じる。

●転職者の受入れ時
・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。
・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。またそうした社員は、自社を辞める時も同じような行動を次の就職先に対して行うリスクを持っている可能性も考えられる。
・競合他社社員を採用する場合に、前職との間で如何なる営業秘密に関して秘密保持義務を課せられているかを事前に確認する。
・採用の際に、前職の営業秘密を使用又は開示しないことを誓約させる。

●金型図面等の授受時[7]

金型図面等の接受については、当事者間において金型図面等の権利関係が明確にされないまま接受が行われるケース、金型ユーザー側に守秘義務がかけられていないケースがあり、一部のユーザーは金型図面等の権利を取得したものと一方的に解釈して、当該金型図面等をもとに海外の金型メーカーに、類似の金型を製造委託している例なども存在する。

これは、金型メーカーの多くは中小企業であり、下請受注型の形態をとっているため、将来、ユーザー（発注者側）との取引を失うことに対するおそれから、取引に当たって正当な権利を主張しにくい心理的状況に置かれていることがその一因となっており、こうしたケースには特に注意して対応する必要がある。

この点については、金型メーカー側だけでなく、曖昧な契約のまま金型図面等を接受した側が、後に何らかの責任を問われることがないよう注意する必要がある。

・金型の取引に当たっては、契約の実態を正確に反映した契約書を締結する。
・金型図面等には、金型メーカー及びユーザー両方のノウハウ等が含まれている場合が多いため、ノウハウ等の帰属については、両当事者の知的貢献度を十分踏まえた上で、契約書において明確化する。
・金型図面等の授受により、相手側のノウハウ等を知り得る場合には、当該ノウハウ等に関して、秘密保持契約を締結する。

各種情報に対する厳格な管理を行うため、社内における営業秘密や個人情報等を一元的に管理する専門の部門等を設置し、これを独立させることも考えられる。

[7]平成 14 年 7 月に「金型図面や金型加工データの意図せざる流出の防止に関する指針」（平成 14・06・12 製局第４号　経済産業省製造産業政策局長、商務情報政策局長通知）が公表されている。

（ウ）　周知徹底、教育

従業者等による適切な責務の実施を期待するためには、どのように行動すべきか等について適切な周知・教育・研修を行い、前述の管理方針等や、各種手続きを従業者に周知徹底することが重要である。

ただし、教育・研修は、全従業者を対象にした教育のみでなく、職場や職務ごとのリスク・責務に応じたものを行うことが望まれる。また、企業側からみた営業秘密保護の観点だけではなく、従業者保護の観点から、従業者が営業秘密侵害罪に問われないための自衛手段等についても予防立証を含めた教育・研修を行うことが望ましい。

＜具体的対応例＞

○一般従業者に対し、営業秘密についての周知・徹底を図る。

・イントラネット等を通じた法律、基本方針及び行動計画、他社の営業秘密の取扱い方法等を周知する。

・上記内容に関する研修を行う。

・なおその際、転職者の自衛の手段として、転職者やその予備軍に対して処罰されないための予防立証を含めた研修を行う。

具体的には、前述の「ペーパートレイル」や、「クリーン・ルーム」などの方法についても周知していくことに加え、従業者が非常に不利益を被る競業避止契約は無効であるということなど、従業者側の保護に資する内容についても研修を行う。

○営業秘密に接する可能性が高い者（共同開発従事者、大学等研究機関への出向者、情報収集担当者など）や、担当管理職等に対しては、さらなる教育・研修活動を実施する。

○担当取締役等の情報の取扱責任者は、専門家等のサポートを受け、法律及び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の理解を深める。

（エ）　リスク顕在化への対応

実際に営業秘密の漏えい、流出、営業秘密の取得を基にした脅迫、データベースの破壊等、他社の営業秘密の侵害の懸念、情報のセキュリティに関する事件・事故及び障害等が発生した場合には直ちに状況を把握し、的確な対応を迅速に行う。

＜具体的対応例＞

○あらかじめ定めた連絡網を通じて直ちに報告する。
○経営責任者の指示のもと、事前に設けた方針や規則に沿って、事件事故及び障害への対応を迅速に行い、損害の最小化を図る。
○外部に開示する必要があるものについては、速やかに行う。
○被害企業に対する謝罪・補償等の措置を講じる。
○発生した原因を調査し、その結果を今後の体制見直しに活かす。
○関係者の処分を実施し、その結果を内部で事例として共有し、再発防止に努める。セキュリティに関する罰則規定に該当する場合はその処分を行う。
○是正措置と再発防止措置（再発防止のための予防措置）を講じ、講じた措置の記録をとる。
○報告手順、対応手順を見直した場合は、それを文書化する。
○教育に反映させる。

③　管理状況のチェック（監査、モニタリング）＜check＞

管理の実効性を確認するために、日常的なモニタリングに加え、定期的に内部監査を実施することが重要である。
必要に応じ、外部監査（第二者監査、第三者監査）を実施することが考えられる。

管理の実効性を確認するために、実際行われている管理が、管理方針等に沿って行われているか、秘密管理が有効に行われているか、他社の営業秘密への侵害が生じていないか等について、まずは日常的にモニタリングし、その上で内部監査を定期的に実施することが重要である。

監査に当たっては、あらかじめ監査責任者を設置する等、組織としての監査責任を明確にすることが考えられる。

また、監査責任者には被監査部門から独立した立場にある者を選定して監査の独立性を確保し、同時に監査責任者が秘密情報管理に関する監査を定期的に実施する権限を有する旨、組織内に徹底することが考えられる。

（ア）　日常的なモニタリング

②の管理方針等の実施に関し、日常的に以下のような点に関し、内部的なモニタリングが行われることが重要である。

- それぞれのレベルの責任者の任務の実施状況に関する総括責任者によるチェック
- 社内において相談があった案件に関する整理、分析と対応策の整理
- 社内における周知状況に関する調査及び不足している場合の対応策の検討
- リスクが顕在化したケースの状況及び原因の整理、分析と組織的対応策の整理

（イ）　内部監査

日常的なモニタリングの状況を踏まえ、組織的に営業秘密侵害の発生リスクに応じた内部監査を実施することが重要である（第一者監査）。

第一者監査とは、マネジメントのレビュー、その他の内部目的のためにその企業自身又は代理人によって行われる監査のことである。

リスクに応じた監査とは、一般的には、仕事の性質上、営業秘密の漏洩、侵害の発生可能性が高い職場に対しては、監査の対象とする部署等の範囲を拡大する、

実施する監査手続きのレベルを高める、監査頻度を高める等の対応を実施する一方、それ以外の職場に対しては、それに対応した監査を実施することをいう。

一般には、内部監査のみでは、すべての問題行為を発見することができるとは限らないと考えられているので、例えば、内部部署からの報告等により潜在的な問題が発見された場合、その経験を踏まえて、監査項目や監査対象等を見直し、監査の制度を継続的に改善することが求められる。

監査の結果、改善が必要と判断される場合、監査責任者はその緊急度合いに応じて、被監査部門に対し「是正措置」又は「予防措置」を実施するよう通知し、各々改善を促すことが考えられる。

ここにおいて「是正措置」とは、不適合（管理方針等が実施されていない状態）の原因を除去するための対策をいい、緊急性が高い改善項目に対してなされるのに対し、「予防措置」とは将来起こり得る不適合が発生しないようその原因を除去するための対策で、「是正措置」ほど緊急性が高くない改善項目に対してなされる。

（ウ）　外部監査

内部監査だけでは対応が難しいケースには、外部監査を実施する方法も考えられる。

なお、外部監査には第二者監査と第三者監査がある。第二者監査は、その組織の利害関係者(顧客など)又は代理人によって行われる監査、例えば開示元企業が開示先企業に対して監査を行うものであり、第三者監査は、認証等のように当該企業と利害関係がない第三者の独立した機関の専門家が客観的、専門的に監査を行うものである。

外部監査は、企業の規模等から導入が難しいケースも考えられるが、監査の透明性確保の観点から必要に応じて導入することが重要である。

（エ）　監査結果の記録

最後に、監査の結果を記録として一定期間保存することが望ましいと考えられる。これにより記録に基づいた是正措置や予防措置のチェックが次回の監査時等で可能となり、一層の秘密管理の徹底が図られるものと考えられる。

④　見直し＜act＞

秘密管理の適切性及び有効性、パフォーマンス等を継続して確保するために、監査の結果や秘密管理に関する法令又は社会動向等の変化に応じて、定期的に管理方針等を点検し、その結果をもとにその手段や計画、目標等を見直すことが望ましい。

（ア）　モニタリング、監査結果の活用、分析

モニタリングや監査の結果を的確に分析し、改善が必要と判断された場合、当該問題点が、管理方針等自体に問題があるのか、それともそれが適切に実施・運用されていないことによる問題であるのかを判断し、仮に管理方針等に問題が有ると判断される場合には、適切に見直していくことが必要となる。

（イ）　管理方針等の見直し

監査結果等を踏まえ、従業者の負担の軽減、組織の管理コストの低減といった観点も含め、単に厳格化するのではなく、実効性を高める方策をとるとの観点から、柔軟に管理方針等を見直し、その実効を図ることが重要である。見直しの内容は、組織の経営層によって実施され、又は承認されることが望ましい。

（4）情報管理に関するマネジメント規格、個人情報保護との関係

現在、国内における情報管理に関するマネジメント規格やそれに基づく第三者認証制度には、ISMS 認証基準（情報セキュリティマネジメントシステム適合性評価制度）があげられる。営業秘密との関わりの中では、特に「秘密管理性」を高いレベルにおいて認証する制度として参考になるものと考えられる。

また、個人情報保護法が施行され、顧客情報等の個人情報については、より厳格な管理が求められることになっている。高い秘密管理性を保った営業活動に有益な顧客名簿については営業秘密にも該当し得るため、個人情報保護法の各種ガイドライン等とも整合性をもって、秘密管理を進めていくことが重要である。

これら情報マネジメント規格や個人情報保護法への対応と整合性をもって営業秘密を管理し、統一的な管理体制を構築することにより、情報の種類毎に新たな管理体制を構築することなく、管理コストの低減につながるものと考えられる。