

營業秘密管理指針

平成15年1月30日

平成17年10月12日改訂

平成22年4月9日改訂

經濟產業省

目次

本指針の構成.....	5
第1章 概説.....	6
1. 背景.....	6
(1) 営業秘密保護が求められた歴史的背景(平成2年~).....	6
(2) 営業秘密管理指針の策定等の背景(平成14年~).....	6
営業秘密管理指針の策定等.....	6
営業秘密管理指針の改訂等.....	7
(3) 今般の営業秘密管理指針の改訂等の背景(平成21年~).....	7
平成21年の法改正等.....	7
今般の改訂の方針.....	8
2. 営業秘密の管理の意義・ポイント.....	9
(1) 知的資産経営による競争力向上.....	9
(2) 秘密管理における視座.....	10
(3) コンプライアンスと人的管理.....	11
第2章 不正競争防止法上の営業秘密の保護.....	12
1. 営業秘密の定義.....	12
(1) 秘密管理性(秘密として管理されていること).....	13
(2) 有用性(事業活動に有用な情報であること).....	14
(3) 非公知性.....	14
2. 営業秘密の民事的保護.....	15
(1) 営業秘密に係る「不正競争」の各類型.....	15
第4号.....	15
第5号.....	15
第6号.....	15
第7号.....	15
第8号.....	16
第9号.....	16
(2) 不正競争行為に対する措置.....	17
差止請求権(第3条・第15条).....	17
損害賠償請求権(第4条~第9条).....	17
信用回復措置請求権(第14条).....	18
(3) 民事訴訟における営業秘密の保護.....	18
秘密保持命令(第10条~第12条).....	18
書類の提出等(インカメラ審理)(第7条第2項、第3項).....	18

営業秘密が問題となる訴訟における公開停止（第13条）	18
3. 営業秘密の刑事的保護	19
(1) 営業秘密侵害罪の類型	19
第1号	19
第2号	19
第3号	19
第4号	19
第5号	19
第6号	20
第7号	20
(2) 営業秘密侵害罪に関する留意点	21
主観的要件	21
行為態様	22
(ア) 不正取得	22
(イ) 領得	22
国外犯	24
親告罪	24
両罰規定	24
法定刑	24
第3章 営業秘密を保護するための管理の在り方	25
1. 概要	25
(1) 本章において目指す営業秘密の管理水準等	25
(2) 裁判例にみる秘密管理性の判断の傾向	27
秘密管理性の要件と肯定的な判断要素とされる具体的な管理方法	27
裁判例にみる秘密管理性判断のポイント	28
(3) 営業秘密管理のポイント	29
2. 営業秘密の管理のために実施することが望ましい秘密管理方法	30
(1) 秘密指定、アクセス権者の指定	30
情報の区分・秘密指定	30
アクセス権者の指定	31
(2) 物理的・技術的管理	33
基本的な考え方	33
物理的管理	33
(ア) 秘密表示、分離保管	33
(イ) 媒体の保管、持ち出し、複製の制限、廃棄	36
(ウ) 施設等の管理	38
技術的管理	41
(ア) マニュアル等の設定	41

(イ)	アクセス及びその管理者の特定・限定.....	41
(ウ)	外部からの侵入に対する防御.....	41
(エ)	データの消去、廃棄.....	42
(3)	人的管理.....	45
	基本的な考え方.....	45
	人的管理.....	46
(ア)	従業者等に対する教育・研修の実施.....	46
(イ)	就業規則・契約等による従業者、退職者等への秘密保持の要請.....	48
(ウ)	派遣従業者.....	56
(エ)	転入者.....	57
(オ)	取引先.....	59
(4)	営業秘密侵害に備えた証拠確保等に関する管理.....	63
3.	営業秘密の管理を適切に機能させるために実施することが望ましい組織的管理 の在り方.....	64
(1)	基本的な考え方.....	64
(2)	他社の営業秘密を侵害しないための組織的管理の意義.....	64
	両罰規定と選任監督義務（刑事罰）.....	65
	相当の注意（民事上の措置）.....	65
(3)	望ましい組織的な管理体制の構築の在り方.....	66
	重要な情報資産（営業秘密として管理すべき情報資産）の把握.....	66
	目安となる事項.....	67
(ア)	管理方針等（基本方針、基準、規程等）の整備.....	67
(イ)	責任者の存在とその権限の明確化.....	67
(ウ)	営業秘密侵害を防止するための教育、管理方針等の周知徹底.....	68
(エ)	日常的なモニタリングの実施.....	68
(オ)	内部監査の実施.....	68
(カ)	事後対応体制の整備.....	68
	望ましい組織的管理のポイント（PDCAサイクルの確立）.....	69
(ア)	管理方針等（基本方針、規程、基準等）の策定＜Plan＞.....	69
(イ)	実施（責任者の設置、従業者への周知徹底）＜Do＞.....	71
(ウ)	管理状況のチェック（監査、モニタリング）＜Check＞.....	74
(エ)	見直し＜Act＞.....	75
(4)	営業秘密の管理と情報管理に関する国際規格（マネジメント規格）、個人情報 保護等との関係.....	81

【参考資料】

参考資料 1	営業秘密管理チェックシート
参考資料 2	各種契約書等の参考例
参考資料 3	我が国における情報管理に関する各種ガイドライン等について
参考資料 4	営業秘密を適切に管理するための導入手順について ～ はじめて営業秘密を管理する事業者のために～

本指針の構成

本指針においては、第1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いて説明し、第3章において営業秘密を保護するための管理の在り方について述べている。

また、本指針に基づく適切な営業秘密の管理体制の構築等に資するよう、参考資料として、「営業秘密管理チェックシート」(参考資料1)、「各種契約書等の参考例」(同2)、「我が国における情報管理に関する各種ガイドライン等について」(同3)、「営業秘密を適切に管理するための導入手順について ～はじめて営業秘密を管理する事業者のために～」(同4)を作成しているので、必要に応じて参考とすることが望ましい。

第1章 概説

本章においては、まず、「1．背景」において、これまでの営業秘密の法的保護の段階的な整備・強化を踏まえた本指針改訂の背景事情について説明する。

次に、「2．営業秘密の管理の意義・ポイント」において、事業経営上の営業秘密管理の重要性やその際に考慮すべき観点等について説明する。

1．背景

(1) 営業秘密保護が求められた歴史的背景（平成2年～）

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年代の改正刑法草案における企業秘密漏示罪の実現が見送られた後、国際的な事業展開の増大に伴う事業者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年の法改正では、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」として差止請求、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事業者の競争力を脅かす一方、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事業者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、事業者ごとの個性であり、他社と自社と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より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、その中でも、そのような情報を秘匿化することによって差別化を持続させることができる営業秘密の扱いが注目されるようになった。

(2) 営業秘密管理指針の策定等の背景（平成14年～）

営業秘密管理指針の策定等

平成14年7月、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し、その中には、営業秘密の不正取得等に対する刑事罰の導入¹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」ことが盛り込まれた。経済産業省は、これを受けて、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。

なお、大学が保有・管理する秘密情報については、平成16年4月に、大学が秘密

¹ この点については、平成15年の法改正によって、営業秘密の不正取得等に対する刑事罰が規定された。

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」を策定・公表している（平成 18 年 5 月改訂²）。

営業秘密管理指針の改訂等

知的財産戦略大綱の策定や刑事罰（営業秘密侵害罪）の導入、管理指針の策定等を行った後も、東アジア諸国及び地域、とりわけ中国、韓国、台湾等の技術的な発展が加速し、営業秘密の侵害によって我が国事業者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や、事業者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・元従業員）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、営業秘密の保護の更なる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、平成 17 年の法改正によって、国外犯規定の導入、一定の条件を満たす退職者及び法人に対する刑事罰の導入、罰則規定の法定刑の引上げなどがなされた。この改正を検討する過程では、事業者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、多くの事業者が自社の取り扱う情報を管理する重要性を認識し、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た。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、事業者の営業秘密の管理強化を促したところである。

なお、その後、平成 18 年の法改正によって、罰則規定の法定刑の引上げなどがなされた。

（ 3 ） 今般の営業秘密管理指針の改訂等の背景（平成 21 年～）

平成 21 年の法改正等

平成 18 年の法改正後も、営業秘密侵害罪について、その処罰範囲が過度に限定されており、営業秘密侵害行為に対する適切な抑止力となっていないなどの問題点が指摘されるようになり、同罪の処罰範囲の見直しを求める要望が高まったことなどから、平成 21 年の第 171 回通常国会において、営業秘密侵害罪について、目的要件の変更、営業秘密の不正な取得行為等を原則として刑事罰の対象とすることなどを内容とする法改正がなされた（平成 21 年法律第 30 号）。

この改正を検討する過程において、営業秘密の適正な管理や事業者による理解の促進を図るよう事業者へ周知徹底するための措置を講じること、労働者の正当な行為や日常業務が処罰対象とならないことを指針等により明確に示すこと、中小企業が保有する営業秘密が不当に流出することのないよう、中小企業の実態に即した適切な措置を講じること、下請企業の営業秘密侵害の防止の在り方について早急な検討を行い、適正な措置を講じることが必要であるとの指摘があった³。

² 平成 17 年の法改正（法改正の内容については後記 を参照。）を受けて、同ガイドラインも改正内容に対応した想定事例を追加する等の改訂を行っている。

³ 第 171 回通常国会における衆・参両院による審議及び附帯決議等

今般の改訂の方針

以上の指摘を踏まえ、経済産業省は、以下の方針に基づき、営業秘密管理指針を再度改訂し、事業者が保有する重要な情報につき、不正競争防止法上の営業秘密としての保護を受けることができるようにするため、事業者に対して営業秘密の適切な管理を促すこととした。

） 平成 21 年の法改正における処罰対象行為の明確化

平成 21 年の法改正の趣旨が適切に理解されるようにするため、処罰対象となる行為類型等を具体的に明らかにする。

） 事業者の実態を踏まえた合理性のある秘密管理方法の提示

不正競争防止法上の営業秘密としての法的保護を享受するためには、事業規模や情報の性質等に応じた合理性のある秘密管理を行うことで足りることを明確にするとともに、営業秘密と認められ得るための管理方法と、漏えいリスクを最小化するための高度な管理方法とを分けて具体的に列挙する。

） 中小企業等における管理体制の導入手順例や参照ツールの提示

主に中小企業等を対象として、適切な管理体制を構築するための導入手順例を紹介するとともに、営業秘密管理チェックシートや各種契約書の参考例等の参照ツールを提示する。

各事業者においては、今般の改訂を踏まえた営業秘密管理指針を参考として、自社における他社との優位性のある技術やノウハウなどを明確に認識し、どの情報資産をどの程度のコストをかけて秘密として管理するかについて、自社の事業構造や事業規模、提供製品・役務の市場環境・最終需要者の市場動向に加え、秘密として管理すべき情報資産の性質・内容等を踏まえ、戦略的で実効的な管理とすべく判断することによって、適切な経営が行われることを期待したい。

2. 営業秘密の管理の意義・ポイント

(1) 知的資産経営による競争力向上

競争力の維持又は強化のためには、無形の経営資源である技術やノウハウなどを自社の強みとして経営者が的確に把握した上で適切に活用し、他社との差別化を行う知的資産経営が求められる。

営業秘密を適切に管理することは、その差別性を持続させることを可能とするものであり、経営戦略の一部として行うことが重要である。

知識集約型経済の急速な発展に伴い、事業活動において、その競争力の維持又は強化のために、無形の経営資源である技術やノウハウなどの知的資産の創出、管理、活用、結合等を重視した経営方法やビジネスモデルの構築がますます重要になってきている。これらの知的資産は、それぞれの事業者固有のものであり、また、それを組み合わせる方法が新たな価値を生み出す力となるものであって、その方法を他社が単純に模倣することは困難である。経営者においては、これまで以上にその重要性を理解した上で、まずは自社の強みや価値の作り方、それらの源泉となっている知的資産を把握し、自らの経営の在り方をその目で再確認することによって、それらを最大限に活用した経営（「知的資産経営」）を実践していくことが重要である。

本指針において述べる営業秘密管理の考え方は、自らの競争優位の源泉を正確に理解し、それを内部で適切に管理することを出発点とするものであるから、こうした知的資産経営の考え方と一致しており、当該管理はまさに知的資産経営の一部として行われるものであるといえる。加えて、営業秘密を適切に管理することは、経営上、資金調達の観点からも有効である⁴。

さらに、財務報告のみでは十分に表せない企業価値を表現するツールとして知的資産等を含む非財務情報の開示が重要であることからすると、営業秘密を適切に把握、管理することは、同時に開示可能な情報を精査することにもつながるため、営業秘密の管理は情報開示の観点からも有効であると考えられる。

また、営業秘密として管理される知的資産の多くは、事業活動を支える現場の労働者や技術者の長年の努力と事業者の多額の投資の結集であり、事業者の収益を生み出す源としての価値を有しているとともに（根源性）、一度侵害されてしまうと瞬時に拡散し、その回復が極めて困難となり（不可逆性・回復困難性）、また、人的・組織的な管理によらざるを得ないことから、侵害行為の予防には限界があるという性質を内包している（予防困難性）。したがって、事業者においては、このような特性をよく理解した上で、刻々と変化する事業環境を適切に把握し、それに適応する視点をもって、自社の強みを明確に把握し、経営者の経営理念とリーダーシップの下で持続的な利益を得るための戦略的な経営資源の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などの意図しない流出等を防ぐことで、自らの投資の成果に他社の追随を許さない状況を実現す

⁴ 例えば、取引先企業の不動産担保や個人保証等に過度に依存することなく、定性的な非財務要素の適正な評価を行っていると考えられる金融機関においては、融資額の変更に影響を与える非財務情報第2位に「営業秘密の漏えいリスクへの対応」を挙げている（独立行政法人中小企業基盤整備機構「中小企業のための知的資産経営実践の指針～知的資産経営ファイナンス調査・研究編～」参照。）

ることが重要である。強みの源泉となる技術やノウハウなどの意図しない流出等を事前に防ぐ手段として、とりわけ特許権等の権利取得になじまない重要な情報資産については、事業者内部において営業秘密として管理し、活用することも有効である。また、特許権等の権利取得が可能である場合であっても、出願公開によって情報の内容が公になることなどを考慮して、営業秘密としての活用を選択することも考えられる⁵。

さらに、我が国事業者が激化する国際競争を勝ち抜いていくためには、自社の技術やノウハウなどに加え、組織外部のそれをも活用しつつ、新しい価値やビジネスモデルの創造を実現するというオープンイノベーションの促進が求められている。そして、このようなオープンイノベーションを実現するためには、事業者間で相互に営業秘密に相当する競争力の源泉を開示しなければならないことから、その前提としても、営業秘密管理の徹底は重要である。また、具体的な実現の機会に当たっては、自社の製品やサービスの共有、普及のために他社に使用させる部分と、利益の確保のために他社に使用させない部分を決定する必要があるところ、このような場合には、他社に使用させる部分については、特許権等を取得してライセンス契約を行う方法等が考えられ、また、他社に使用させない部分については、特許権等を取得するがライセンス契約は行わない方法や営業秘密として管理する方法が考えられる。

(2) 秘密管理における視座

秘密情報が漏えいした場合に、事後的に法的保護を受けることができる実効的な管理をすることが望ましいと同時に、漏えいリスク・管理コスト・業務効率のバランスを考慮した合理的な管理をすることが重要である。

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である秘密管理性の重要な要素となるため、営業秘密としての法的保護を受けるための前提条件である。また、いかに重要な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いければ、営業秘密としての法的保護を受けることはできない。

そこで、事業者においては、秘密情報が漏えいした場合に、事後的に法的保護を受けることができる実効的な管理をすることが望ましい。

ただし、事業者の保有する多くの情報を適切に管理することは重要であるが、大量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のみならず、管理の実効性や業務効率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いことにもなりかねない。

このため、事業者は、営業秘密として管理すべき情報を経営・事業戦略との整合性等を踏まえて絞り込んだ上で、漏えいリスク・管理コスト・業務効率のバランスを考慮した合理的な管理をすることが重要である。

⁵ なお、特許権として保護され得る情報資産（発明）をノウハウとして秘匿することを選択した場合は、発明を実施している（事業を行っている）又はその準備をしていれば、その後、他社が特許権を取得したとしても、無償の通常実施権が得られる制度、いわゆる先使用权制度が設けられており、当該制度を活用することにより、事業者は継続的に事業実施を行うことが可能である。先使用权については、「先使用权制度の円滑な活用に向けて - 戦略的なノウハウ管理のために -」（平成 18 年 6 月特許庁）を参照されたい。

(3) コンプライアンスと人的管理

コンプライアンスの観点から、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することが必要である。

また、従業者を萎縮させることのない適切な管理をすることが求められる。
さらに、営業秘密管理の実効性を高めるためにも「人」の管理が重要である。

前記「1. 背景」において述べたように、営業秘密を巡る背景事情の変化に対応するべく、不正競争防止法の改正が段階的になされたことにより、営業秘密を侵害する行為に対する法的保護が整備・強化された結果、営業秘密侵害罪を犯した者のみならず、その者が所属する事業者の刑事的責任が問われる可能性が存在するようになった。

すなわち、事業者は、自社の情報を保護することのみならず、他社から開示された営業秘密も保護することや、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。コンプライアンスが重視される昨今においては、「自社の従業者が、他社の営業秘密を侵害しない」ための管理をすることの必要性が、自社の営業秘密の漏えい防止の必要性とともに増大している。

これらの観点から、秘密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、営業秘密を扱う「人」の管理を行うことが重要である。

「人」の管理においては、罰則等で威嚇しながら全ての従業者等（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方法を用いた場合、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なく、かえって管理が非効率になることがある。このような事態を避けつつ、管理の実効性を向上させるためには、どの情報にどの従業者が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に対して適切な管理を行うことが重要である。また、物理的・技術的管理のみによって、どれほど厳格に管理しようとしたとしても、私的な欲望や周囲に対する不満等がきっかけで不正行為がなされることがあり、これを完全に防止することは難しい。そこで、このような不正行為をできる限り予防するためにも、平時から上司や先輩、同僚とのコミュニケーションが円滑に行われているかなども配慮した「人」の管理を行うことが重要である。また、このような「人」の管理を行うに当たっては、公益通報者保護法等他の法制度と整合性をもって行うことが望まれる。

以上のように、事業者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えい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。

第2章 不正競争防止法上の営業秘密の保護

本章においては、まず、「1．営業秘密の定義」において、不正競争防止法による保護を受けることができる「営業秘密」の定義とともに、営業秘密として認められるために必要な三要件（秘密管理性、有用性、非公知性）について説明する。

次に、「2．営業秘密の民事的保護」において、不正競争防止法上「不正競争」と定義されている営業秘密の不正な取得行為等の行為類型と、それに対する民事的措置（差止請求権、損害賠償請求権、信用回復措置請求権）民事訴訟における営業秘密の保護措置（秘密保持命令、インカメラ審理、当事者尋問等の公開停止）について説明する。

さらに、「3．営業秘密の刑事的保護」において、営業秘密侵害罪に該当する行為類型とその留意点について説明する。

1． 営業秘密の定義

「営業秘密」とは、秘密として管理されていること、有用な情報であること、公然と知られていないことの三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。

不正競争防止法第2条第6項（以下、単に条項のみを記載するときは不正競争防止法のそれを指すこととする。）は、営業秘密を「秘密として管理されている〔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〔有用性〕であって、公然と知られていないもの〔非公知性〕をいう。」と定義しており、この三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、不正競争防止法上の「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、上記三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、情報にアクセスできる者を特定すること、情報にアクセスした者が、それを秘密であると認識できること、の二つが要件となる。

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、当該情報にアクセスできる者を制限するとともに、同情報にアクセスした者にそれが秘密であることを認識できるようにしていることが必要とされている⁶。

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、記憶されて持ち出された当該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、その不正な使用行為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い場合は、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⁷

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わけではない。例えば、いたずらに「秘」のスタンプを押印したような場合においては、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、営業秘密の要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。

⁶ 東京地裁平成12年9月28日判決

⁷ この点を踏まえ、実務においては、これを可視化して管理可能にしようと努める向きもある。

(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。

一方、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ったりするものであることを意味し(事業への活用性)、裁判例では、「財やサービスの生産、販売、研究開発に役立つなど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⁸。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)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でなく、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、有用性の有無が異なる場合もあり得る。

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等を教示し、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、営業秘密としての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など、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、非公知情報とはいえない。

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、非公知情報といえる。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など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、非公知情報であると考えられる。

⁸ 東京地裁平成14年2月14日判決

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、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、営業秘密に係る不正行為を列挙して、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。

第4号

保有者から、営業秘密を窃取・詐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、セラミックコンデンサー積層機及び印刷機的设计図の電子データを無断で複製し、これを使用・開示する行為⁹等がこれに当たる。

第5号

第4号の不正取得行為の介在について悪意又は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員から、産業スパイが、不正に取得されたことを知りながら当該機密文書を受け取る行為等がこれに当たる。

第6号

第三者が、不正取得行為の介在について善意かつ無重過失で営業秘密を取得した後、悪意又は重過失に転じた上で、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、当該営業秘密に係る産業スパイ事件が大々的に報道されるなどして不正取得行為が介在していた事実を知ったにもかかわらず、あえて営業秘密を使用し、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。）

第7号

営業秘密の保有者が従業員、下請企業、ライセンサーなどに対して営業秘密を示した場合に、その従業員等が、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。「不正の

⁹ 大阪地裁平成15年2月27日判決

利益を得る目的」とは、競争関係にある事業を行う目的のみならず、広く公序良俗又は信義則に反する形で不当な利益を図る目的のことをいう。これには、自ら不正の利益を得る目的（自己図利目的）のみならず、第三者に不正の利益を得させる目的（第三者図利目的）も含まれる。「保有者に損害を加える目的」とは、営業秘密の保有者に対し、財産上の損害、信用の失墜その他の有形無形の不当な損害を加える目的のことを指し、現実には損害が生じることは要しない。例えば、学習器具並びに出版物の製作及び販売等を営業目的とする株式会社の代表取締役が、在職中に、従業者に依頼して顧客情報をフロッピーディスクにコピーさせた上、従業者からそれを受け取って自宅に持ち帰り、退職後に、不正の利益を得る目的等で当該顧客情報を用いて転職先企業において販売を開始する行為¹⁰等がこれに当たる。

第 8 号

営業秘密を取得する際に、不正開示行為（保有者から営業秘密を示された場合において、図利加害目的をもって、若しくは守秘義務違反により、その営業秘密を開示する行為）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、悪意若しくは重過失で、営業秘密を取得する行為、又はその取得した営業秘密を使用し、若しくは開示する行為である。例えば、人材派遣事業等を主たる営業目的とする株式会社の従業者から、当該会社が保有する派遣スタッフの管理名簿等の不正開示を受け、そのことを知りながら当該名簿等を使用して勧誘等する行為¹¹等がこれに当たる。

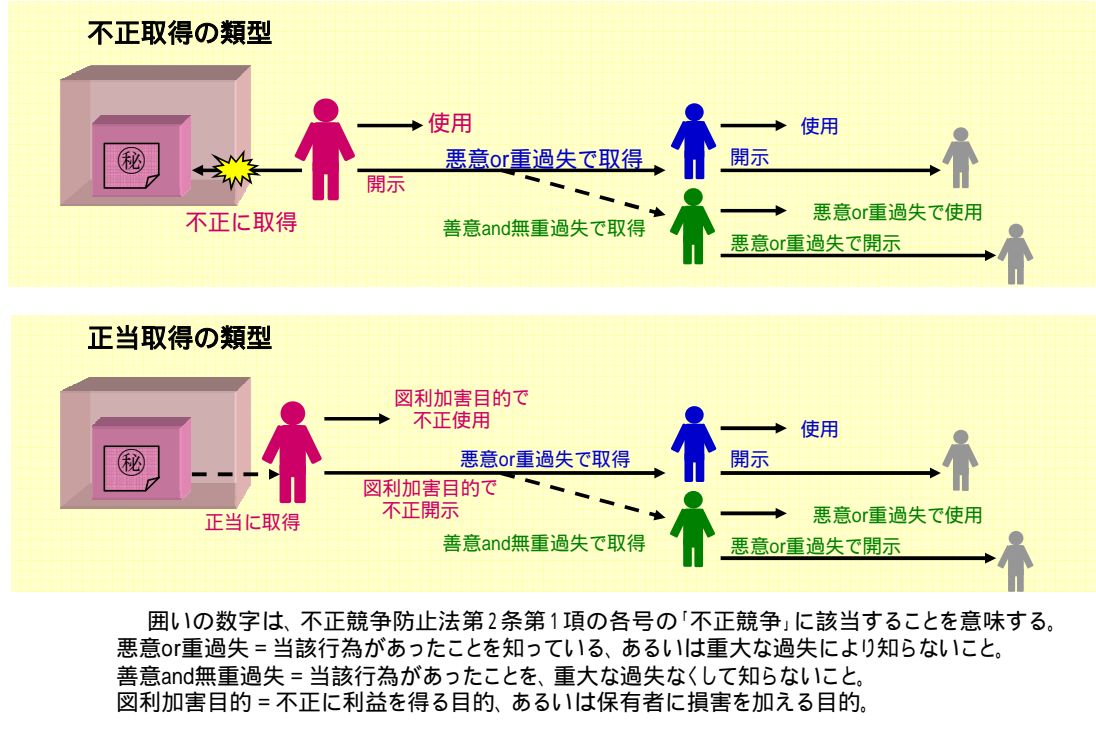
第 9 号

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、又は不正開示行為が介在したことについて、悪意又は重過失で、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ったにもかかわらず、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。）

¹⁰ 東京地裁平成 16 年 5 月 14 日判決

¹¹ 東京地裁平成 14 年 12 月 26 日中間判決

営業秘密侵害行為類型



(2) 不正競争行為に対する措置

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（第3条第1項）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（第3条第2項）を請求することができる。

なお、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）

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、(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)×(侵害者が譲渡した物の数量)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)

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

営業秘密侵害に対する差止請求や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えいするのを恐れ、その提出が困難な場合もある。こうしたことなどのため、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。

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、その請求後直ちに、同項の申立てをした当事者に対し、その請求があった旨を通知しなければならない。これにより、通知を受けた当事者は、請求手続を行った者に対する秘密保持命令の申立てができることとなる。

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。

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・領得(これらの意義については後掲(2)(ア)・(イ)を参照。)、不正使用・不正開示のうち、一定の行為について、10年以下の懲役又は1000万円以下の罰金(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処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犯罪)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1号から第7号までにおいて、営業秘密侵害罪に該当する七つの類型を規定している。(各類型の要件の解釈等留意すべき点については、後掲(2)参照。)

第1号

不正の利益を得る目的で、又は保有者に損害を加える目的で、詐欺等行為又は管理侵害行為により営業秘密を不正に取得する罪

第2号

詐欺等行為又は管理侵害行為により不正に取得した営業秘密を、不正の利益を得る目的で、又は保有者に損害を加える目的で、使用し、又は開示する罪

第3号

営業秘密を示された者が、不正の利益を得る目的で、又は保有者に損害を加える目的で、その営業秘密の管理に係る任務に背いて、有体物に記録されるなどした営業秘密を領得(有体物の横領、データの不正な複製、データを消去する義務に違反して消去したように仮装することなどを方法とした場合に限る。)する罪

第4号

営業秘密を示された者が、その営業秘密の管理に係る任務に背いて、第3号の方法により領得した営業秘密を、不正の利益を得る目的で、又は保有者に損害を加える目的で、使用し、又は開示する罪

第5号

営業秘密を示された役員又は従業者が、不正の利益を得る目的で、又は保有者

に損害を加える目的で、その営業秘密の管理に係る任務に背いて、その営業秘密を使用し、又は開示する罪

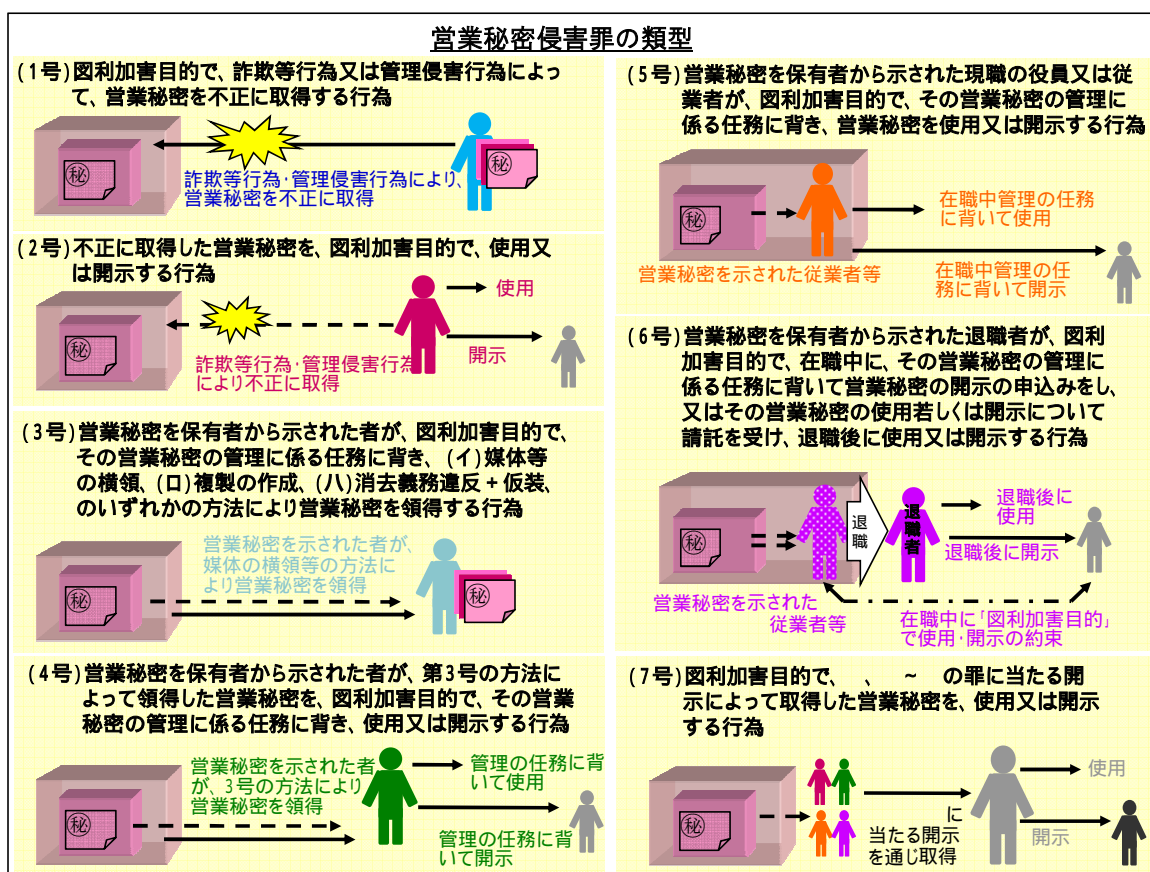
第6号

営業秘密を示された役員又は従業者であった者が、不正の利益を得る目的で、又は保有者に損害を加える目的で、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

第7号

不正の利益を得る目的で、又はその保有者に損害を加える目的で、上記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5号及び第6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。



* 本指針における営業秘密侵害罪に係る記述は、平成21年の法改正後の規定を前提とするものであるところ、同改正法は、平成21年4月30日から起算して1年6月を超えない範囲内において政令で定める日から施行されることとされており、同施行日前の行為については、改正法は適用されず、改正前の不正競争防止法が適用される。

(2) 営業秘密侵害罪に関する留意点

主観的要件

処罰範囲を明確に限定するため、各号ごと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」(以下「図利加害目的」という。)と規定されている。

「不正の利益を得る目的」とは、公序良俗又は信義則に反する形で不当な利益を図る目的のことであり、自ら不正の利益を得る目的(自己図利目的)のみならず、第三者に不正の利益を得させる目的(第三者図利目的)も含まれる。

「保有者に損害を加える目的」とは、営業秘密の保有者に対し、財産上の損害、信用の失墜その他の有形無形の不当な損害を加える目的のことであり、現実には損害が生じることは要しない。

なお、第7号(二次的取得者による営業秘密の不正使用・不正開示)については、取得の時点から目的要件を満たさなければ同号の構成要件に該当せず、営業秘密侵害罪は成立しない。

【図利加害目的に当たる事例】

金銭を得る目的で、競業企業以外に営業秘密を不正に開示する行為

保有者の営業秘密を、自ら不正に使用して不当に収益を上げる目的(自己図利目的)や、開示した者に不正に使用させることによって、その者に不当な収益を上げさせる目的(第三者図利目的)は、営業秘密の保有者と自己又は第三者とが競争関係にある必要はない。

保有者に営業上の損害を加えるため又はその信用を失墜させるため、営業秘密をインターネット上の掲示板に書き込む行為

財産上の損害、信用の失墜その他の有形無形の不当な損害を加える目的は「保有者に損害を加える目的」に当たり、また、現実には損害が生じることを要しない。

外国政府を利用する目的で、営業秘密を外国政府関係者に不正に開示する行為

保有者の営業秘密を、自ら不正に使用して不当に収益を上げる目的(自己図利目的)や、開示した者に不正に使用させることによって、その者に不当な収益を上げさせる目的(第三者図利目的)は、営業秘密の保有者と自己又は第三者とが競争関係にある必要はなく、第三者には外国政府も含まれ得る。

【図利加害目的に当たらない事例】()

なお、下記【図利加害目的に当たらない事例】は、営業秘密侵害罪の構成要件としての図利加害目的に該当しないというにとどまり、各企業における社内規程の違反行為となったり、民事責任の対象となったりする可能性があることは別論である。

公益の実現を図る目的で、企業の不正情報を内部告発する行為

そもそも内部告発の対象となる事業者の不正な情報は、「営業秘密」としての法的保護の対象とならない。また、仮に内部告発のために入手した情報が直ちに不正情報とはいえ、営業秘密と認められるものであったとしても、内部告発は社会公共の利益の増進という公益を図ることを意図するものであるから、このような場合には「不正の利益を

得る目的」には当たらない。また、「損害を加える目的」にいう「損害」は、営業秘密の使用・開示等によって生じる保有者の財産・利益上の損失が公序良俗又は信義則上不当なものといえる場合に限られるから、正当な内部告発行為によって生じた当該企業の損失はそれに当たらない。したがって、正当な内部告発をする者が営業秘密の開示等によって保有者に財産・利益の減少が生じ得ることを認識していたとしても、そのことから直ちに加害目的に当たるとはいえないものと考えられる。

労働者の正当な権利の実現を図る目的で、労使交渉により取得した保有者の営業秘密を、労働組合内部（上部団体等）に開示する行為

従業者の正当な業務活動の一環としてなされた行為については、使用者から許された正当な業務活動であるから、そもそも「営業秘密の管理に係る任務」に背く行為であるとはいえない上、正当な業務を遂行する意図によるものであるから図利加害目的に当たらない。労働組合内部における情報共有行為については、労働者の正当な権利保護等のための組合活動の一環として行われる情報共有等を意図した行為である限り、図利加害目的には当たらないものと考えられる。

残業目的で、権限を有する上司の許可を得ずに、営業秘密が記載等された文書や CD-ROM を自宅に持ち帰る行為

使用者の明示の許可を得ずに営業秘密が記載された書面等を持ち帰った場合であっても、保有者の業務を遂行するために自宅等で残業をする意図にすぎないときは、同様に、図利加害目的には当たらない。

行為態様

（ア） 不正取得

営業秘密侵害罪における不正取得（第1号、第2号）とは、詐欺等行為又は管理侵害行為によって、自己又は第三者が、営業秘密を知得すること又は営業秘密記録媒体等若しくは営業秘密が化体された物件を占有することをいう。例えば、営業秘密を知っている者を欺いてその内容を聞き出す行為や、不正アクセスによって営業秘密である顧客データを視認により記憶する行為等、媒体の取得又は媒体の記録等の複製によらない方法を用いた詐欺等行為又は管理侵害行為による営業秘密の不正取得も、営業秘密侵害罪の対象となる。

（イ） 領得

営業秘密の領得（第3号）とは、営業秘密を保有者から示された者が、その営業秘密を管理する任務に背いて、権限なく営業秘密を保有者の管理支配外に置く意思の発現行為をいい、不正競争防止法は、領得の方法として、営業秘密記録媒体等又は営業秘密が化体された物件を横領する行為（同号イ）、営業秘密記録媒体等の記載若しくは記録について、又は営業秘密が化体された物件について、その複製を作成する行為（同号ロ）、営業秘密記録媒体等の記載又は記録であって、消去すべきものを消去せず、かつ、当該記載又は記録を消去したように仮装する行為（同号ハ）を規定している。

営業秘密の領得は、「営業秘密の管理に係る任務」に反することを前提とするところ、この「営業秘密の管理に係る任務」とは、「営業秘密を保有者から示された者」が、保有者との委任契約又は雇用契約において一般的に課せられた秘

密を保持すべき任務、ないし秘密保持契約等によって個別的に課せられた秘密を保持すべき任務を意味する。この任務を負っている限り、保有者から営業秘密を開示された者は、その立場（在職者・退職者・取引先）にかかわらず、いずれも本罪の主体となり得る。

【領得に当たる事例】

図利加害目的で、営業秘密が記録されたファイルであって持ち出しが禁止されたものを無断で外部に持ち出す行為

「横領」(第3号イ)とは、保有者から預かった営業秘密が記録されるなどした有体物を自己の物のように利用・処分する(ことができる状態に置く)ことをいう。

図利加害目的で、営業秘密が記録されたデータであって複製が禁止されたものを無断でコピーする行為

「複製を作成する」(第3号ロ)とは、印刷、撮影、複写、録音その他の方法により、営業秘密が記載若しくは記録された記録媒体の記載若しくは記録又は営業秘密が化体された物件と同一性を保持するものを有形的に作成することをいう。

図利加害目的で、プロジェクト終了後のデータ消去義務に違反して営業秘密を消去せずに自己のPCに保管し続け、保有者からの問い合わせに対して、消去した旨の虚偽の回答をする行為

「消去すべきものを消去せず」(第3号ハ)とは、保有者から営業秘密を示された者が、当該営業秘密を消去すべき義務に違反して消去しないことをいう。また、「当該記載又は記録を消去したように仮装すること」とは、自己の記録媒体に記録されるなどした営業秘密の記録等を消去した旨の書面を交付する行為のように、実際には記録等を消去していないにもかかわらず、既に消去されているかのような虚偽の外観を作出することをいう。

【領得に当たらない事例】()

なお、下記【領得に当たらない事例】は、営業秘密侵害罪の構成要件としての領得行為に該当しないということにとどまり、各企業における社内規程の違反行為となったり、民事責任の対象となったりする可能性があることは別論である。

権限を有する上司の許可を受け、営業秘密をコピーしたり、営業秘密が記載された資料を外部に持ち出したりする行為

「営業秘密を領得」(第3号柱書)とは、営業秘密を保有者から示された者が、その営業秘密を管理する任務に背いて、権限なく営業秘密を保有者の管理支配外に置く意思の発現行為をいい、権限を有する上司の許可を受けた正当な業務行為はこれに当たらない。

将来、競業活動に利用するかもしれないと思いつつ、媒体を介することなく営業秘密を頭のみで記憶する行為

営業秘密を頭で記憶する行為は、領得の方法として定められた、営業秘密記録媒体等又は営業秘密が化体された物件を横領する行為(第3号イ)、営業秘密記録媒体等の記載若しくは記録について、又は営業秘密が化体された物件について、その複製を作成する行為(同号ロ)、営業秘密記録媒体等の記載又は記録であって、消去すべきものを消去せず、かつ、当該記載又は記録を消去したように仮装する行為(同号ハ)のいずれにも当たらない。

将来、競業活動に利用するかもしれないと思いつつ、プロジェクト終了後のデータ消去義務に反して営業秘密を消去し忘れ自己の PC に保管し続けていたが、保有者からの問い合わせを受け、その後にデータを消去する行為

営業秘密記録媒体等の記載又は記録であって、消去すべきものを消去しない行為は、それ自体では領得の方法（第 3 号八）に当たらず、当該記載又は記録を消去したように仮装する行為があってはじめて第 3 号八に当たる。したがって、「プロジェクト終了後、過失により、USB メモリに記録された営業秘密を消去し忘れる行為」も、消去義務に違反する故意がない上、そもそも仮装する行為がないので、処罰対象行為の類型にも当たらない。

国外犯

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不正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不正開示が行われた場合と同様に処罰の対象となる。

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、営業秘密がその手続の過程で更に開示されることを避けるためである。

両罰規定

不正競争防止法第 22 条の規定により、法人等の代表者、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一定の種類の営業秘密侵害罪（第 1 号、第 2 号、又は第 7 号）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。

なお、法人処罰の規定については、法人等の過失を推定する最高裁判例¹²に照らすと、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いえるような企業としての取組みが必要になる。

法定刑

営業秘密侵害罪の法定刑は、10 年以下の懲役又は 1000 万円以下の罰金であり、懲役刑と罰金刑とを併せて科すことができる。また、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 1 号、第 2 号、又は第 7 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に 3 億円以下の罰金が科され得る。

¹² 最高裁昭和 40 年 3 月 26 日判決

第3章 営業秘密を保護するための管理の在り方

本章においては、まず、「1. 概要」において、営業秘密の管理の在り方について、本章において目指す管理水準の考え方を踏まえるとともに、裁判例における秘密管理性の判断の傾向を把握した上で、営業秘密管理のポイントを示す。

次に、「2. 営業秘密の管理のために実施することが望ましい秘密管理方法」において、営業秘密の管理方法として、秘密指定・アクセス権者の指定、情報自体の物理的・技術的管理、取り扱う人の管理、更には他者（他社）情報（以下「他社情報」という。）の不正な取得・使用の防止等を含め、これらの管理をシステムとして行うための組織的管理について、秘密管理性に関する裁判例において肯定的な要素として考慮されたものを含め、それぞれ事業者一般に採用し得る具体的な管理方法の具体例を示すとともに、併せて、営業秘密の流出を可及的に防ぐこと（漏えいリスクの最小化）などを目的として、更に情報セキュリティレベルの高い管理水準を達成しようとする事業者にとって参考となる高度な管理方法等も紹介する。

1. 概要

(1) 本章において目指す営業秘密の管理水準等

営業秘密の管理は、どのような保護、成果を求めるかによって、それに必要な水準が異なる。

本章では、まず、不正競争防止法上の営業秘密として法的保護を享受し得る情報管理水準を示すことを目指すこととし、その上で更に高いセキュリティレベルを求める事業者の参考となるよう、高度な管理方法等をも紹介する。

なお、不正競争防止法上の営業秘密として法的保護を享受し得る情報管理水準を達成するためには、本章で紹介する管理方法をすべて実践しなければならないものではなく、事業者においてその情報を合理的に管理していることで足りることに留意する必要がある。

事業者が、競争力を維持・強化するという利益を実現していくためには、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じ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。そして、営業秘密の管理は、管理の対象とすべき情報資産・人を明確にしつつ適切に行うべきであって、そのような明確性に欠ける漠然とした管理体制や、いたずらに厳重な管理方法・管理体制を形式的に整えることよりも、事業規模、営業秘密の性質、取り扱う人の範囲、取扱状況、保管場所等に照らして、どのような管理方法・管理体制であれば実効的に管理することができるかということに重視すべきである。

すなわち、事業者が、管理の対象となる情報資産やそれを取り扱う人について、明確に認識すれば、実効的な管理体制を構築・実施することが可能になり、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。他方で、事業者が、管理の対象とするべき情報資産やそれを取り扱う人を明確に認識することなく、だれがどの情報をどのように管理すべきかについてあいまいかつ漠然とした営業秘密管理に取り組んだ場合や、いたずらに厳重な管理を要求し、現場において実践することが困難な営業秘密管理に取り組んだ場合には、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。

一方で、このように情報資産やそれを取り扱う人を特定した上で具体的な管理方法を組み合わせた管理体制を構築・実施することは、情報資産や取扱者の把握、体制整備、具体的な管理方法の導入、実施について、事業者の規模や導入、実施する管理方法等に応じて一定のコスト（金、人、時間）を要する。そして、情報資産の管理によって求めるべき成果としては、一般的に有効な契約に基づく保護を受けることができること、不正競争防止法上の「営業秘密」として保護を受けることができること、それらを超えて現実には漏えいのリスクが極めて小さいという理想的な管理体制を構築することなどが考えられるところ、これらはその求めるべき成果によって、必要とされる情報資産等の特定や講じるべき管理の程度、水準が異なる点に注意する必要がある。そこで、事業者においては、自らの情報資産を管理するに当たり、どのような保護、成果を求めるかを考慮した上で、その管理体制を構築することが望ましい。

本章においては、不正競争防止法上の営業秘密として、侵害者に対して民事上の措置を講じることや刑事罰による制裁を可能とするための適切かつ合理的な情報管理水準を示すことを目指している。

そのため、情報自体の物理的・技術的管理、取り扱う人の管理、更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、それぞれ具体的な管理方法の例を示すが、不正競争防止法上の営業秘密として保護を受けるためには、本章で紹介する管理方法をすべて実践しなければならないものではなく、事業者においてその情報を合理的に管理していることで足りる。

なお、事業者によっては、その事業規模、業種、競争環境、秘密管理すべき情報資産の性質・重要性等に照らし、当該情報を保護することによって事業者が競争力を維持・強化していくためには、不正競争防止法上の保護に値する管理水準に到達することのみを目的とするのではなく、当該情報の流出を可及的に防ぐこと（漏えいリスクの最小化）や当該情報が流出した際の証拠を確保することをも目的として、更に情報セキュリティレベルの高い管理体制を整備しようとするとも考えられることから、本章ではその目的に資すると考えられる高度の管理方法等も紹介するが、このような高度の管理方法等は、これを講じていない限り営業秘密としての法的保護を受けられないものではなく、また場合によってはセキュリティコストが増加し、事業者にとって過度な負担となる場合があることに留意すべきである。

(2) 裁判例にみる秘密管理性の判断の傾向

裁判例は、営業秘密として不正競争防止法上の保護を受けるための要件(秘密管理性)として、アクセス制限の存在、及び、客観的認識可能性の存在を必要としているが、裁判例で考慮されている具体的な管理方法をすべて実施していることまでを求めているのではなく、事業規模、業種、情報の性質、侵害態様等も踏まえ、秘密管理の合理性を総合的に判断する傾向にある。

事業者においては、具体的管理方法を適切に組み合わせてその管理水準を一定以上のものにするにより、法的保護の可能性を高めることが望ましい。

秘密管理性の要件と肯定的な判断要素とされる具体的な管理方法

裁判例においては、営業秘密として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である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(アクセス制限の存在)
- 2) アクセスした者にそれが秘密であることが認識できるようにされていること
(客観的認識可能性の存在)

を必要としており、全般的な傾向として、以下の三点に着目していると考えられる。

- A. アクセスできる者が限定され、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(アクセス権者の限定・無権限者によるアクセスの防止)
- B. アクセスした者が、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者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(秘密であることの表示・秘密保持義務等)
- 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)

肯定的な判断要素とされた具体的な管理方法としては以下のものが挙げられる。

【Aについて】

- アクセス権者の限定¹³
- 施錠されている保管室への保管¹⁴
- 事務所内への外部者の入室の禁止¹⁵
- 電子データの複製等の制限¹⁶
- コンピュータへの外部者のアクセス防止措置¹⁷
- システムの外部ネットワークからの遮断¹⁸

【Bについて】

- 「秘」の印の押印¹⁹

¹³ 大阪高裁平成14年10月11日判決、前掲東京地裁平成16年5月14日判決

¹⁴ 東京地裁平成11年7月23日判決、福岡地裁平成14年12月24日判決

¹⁵ 前掲東京地裁平成16年5月14日判決、大阪高裁平成17年2月17日判決

¹⁶ 前掲大阪地裁平成15年2月27日判決

¹⁷ 前掲大阪地裁平成15年2月27日判決、前掲東京地裁平成16年5月14日判決

¹⁸ 東京地裁平成17年6月27日判決

¹⁹ 大阪地裁平成8年4月16日判決、前掲東京地裁平成12年9月28日判決、前掲東京地裁平成17年6月27日判決

- 社員が秘密管理の責務を認知するための教育の実施²⁰
- 就業規則や誓約書・秘密保持契約による秘密保持義務の設定等²¹

【Cについて】

- 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²²
- 外部からのアクセスに関する応答に関する周知な手順の設定²³

裁判例にみる秘密管理性判断のポイント

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81件ある²⁴。その中において、秘密管理性を肯定したものは23件である。

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が、事業者の規模や組織形態、情報の保管形態等の状況は多種多様であることから、前記 にみた肯定的な要素になる管理方法をすべて実施していない限り、秘密管理性が否定されて営業秘密として認められないものではない。

他方、肯定的な要素になる管理方法を実施していても、同時に秘密としての管理に否定的な要素もみられ、総合的にみて合理性のある秘密管理とはいえない場合においては、秘密管理性が否定されることもある²⁵。

また、裁判例においては、実際に講じられていた秘密管理方法に加えて、事業規模、業種、高度の秘密性が認められる情報であること（当該情報の性質・内容上、その保有企業の属する業界の一般的な慣行に照らして秘密情報として扱われることが当然とされるもの）、侵害態様、侵害者の属性等の諸般の事情を総合考慮することによって、秘密管理体制の合理性の有無を判断する傾向にあると考えられる。

以上にみたように、裁判例においては、諸般の事情を総合考慮し、合理性のある秘密管理方法が実施されていたか否かという観点から、秘密管理性について判断されているものと考えられる²⁶。

この点、営業秘密を適切に管理しようとする事業者において、侵害態様等の事後的な事情をあらかじめ考慮することは必ずしも容易とはいえない。そこで、事業者においては、具体的な管理方法を適切に組み合わせ、その管理水準を一定以上にすることにより、秘密管理性に関する法的判断における事後的な事情への依存度を軽減させ、営業秘密として法的保護を享受し得る可能性を高くすることが望ましい。

²⁰ 東京地裁平成12年11月13日判決、前掲大阪高裁平成14年10月11日判決、前掲東京地裁平成16年5月14日判決

²¹ 前掲東京地裁平成11年7月23日判決、東京地裁平成17年2月25日判決、前掲東京地裁平成17年6月27日判決、大阪高裁平成20年7月18日判決

²² 前掲東京地裁平成11年7月23日判決

²³ 前掲大阪高裁平成14年10月11日判決

²⁴ 平成22年1月末現在において、最高裁ホームページ等により、経済産業省経済産業政策局知的財産政策室が把握しているものに限る。

²⁵ 大阪地裁平成14年9月26日判決、大阪高裁平成19年12月20日判決

²⁶ 実際の裁判例においては、現実にとられていた管理体制は必ずしも厳重なものではなかったものの、侵害態様や情報の性質等の事情も考慮して、秘密管理性を肯定したと考えられるものが複数存在している（大阪地裁平成19年5月24日判決、名古屋地裁平成20年3月13日判決）。

(3) 営業秘密管理のポイント

営業秘密の管理に当たっては、「物理的管理」、「技術的管理」、「人的管理」等の具体的な管理方法により、秘密情報をその他の情報と区分し、権限に基づきアクセスした者がそれを秘密であると認識して取り扱うために必要な措置を講じるとともに、権限のない者がアクセスすることができないような措置を講じることが必要である。また、具体的な管理方法による管理を適切に機能させるために「組織的管理」をすることが重要である。

前記(2)の裁判例の分析を踏まえると、営業秘密の管理に当たっては、一般的には、秘密情報をその他の情報と区分し、権限に基づきアクセスした者がそれを秘密であると認識して取り扱うために必要な措置〔客観的認識可能性〕を講じるとともに、権限のない者がアクセスすることができないような措置〔アクセス制限〕を講じることが必要である。

また、アクセス制限の存在と客観的認識可能性の存在は別個独立した要素ではなく、アクセス制限に必要な措置を講じると同時にその情報が秘密であるという認識可能性を高めることになり、また、客観的認識可能性を高めるために必要な措置を講じるとは(秘密保持義務を負う)アクセス権限のある者にとって秘密を遵守するように働きかけるものであることから同時にアクセス制限の効果をももつといえる。

そして、「2. 営業秘密管理のために講じることが望ましい秘密管理方法」において詳述するが、具体的に営業秘密を管理するに当たっては、まず、書面や記録媒体等の有体物や電子情報に対する管理である「物理的・技術的管理」を実施することが必要である。また、このような「物理的・技術的管理」に基づき営業秘密を取り扱うのは人(アクセス権者等)であるから、「物理的・技術的管理」を導入するに当たり、取り扱う人の能力や業務効率性に対する配慮の視点を持たなければならない。同時に、取り扱う人に対する秘密保持義務の明確化や秘密保持に関する教育等の「人的管理」も必要となる。さらに、これらの「物理的・技術的管理」、「人的管理」等の具体的な管理方法に基づく秘密管理を適切に機能させるためには、その実効性を担保するための組織的な仕組みとしての「組織的管理」が重要である。

なお、秘密情報を他の情報と区分して、秘密情報として指定するとともに、そのアクセス権者及び取扱方法をも指定し、その旨秘密情報を取り扱う可能性のある従業員等に周知することは、権限に基づきアクセスする者に対して秘密であると認識することを容易にさせ、かつ、指定されたルールに基づくアクセス制限を実効的に行うことを容易にするものといえる。

したがって、事業者においては、「2. 営業秘密の管理のために実施することが望ましい秘密管理方法」を参照にしつつ、事業規模、情報の性質、情報の取扱状況等に照らして適切と考えられる秘密管理方法を採用し、その際、総合的にみて、権限に基づきアクセスした者がそれを秘密であると認識して取り扱うために必要な措置を講じるとともに、権限のない者がアクセスすることができないような措置を講じているといえるような合理的な管理を実現するように配慮することが重要である。

2. 営業秘密の管理のために実施することが望ましい秘密管理方法

(1) 秘密指定、アクセス権者の指定

情報の区分・秘密指定

営業秘密とその他の情報とを区分して管理し、営業秘密として区分した情報については、秘密であること及びその管理方法を指定・周知する。

なお、取引先等から秘密情報の開示を受けている場合には、その秘密情報が自社の営業秘密に混入(コンタミネーション)しないようにする。

まず営業秘密として管理する情報とその他の情報とを区分することが必要である。

その際、自社にどのような情報資産があるかをできるかぎり広く把握し、その中でどの情報資産を営業秘密として管理すべきかを判断することが望ましい。

また、営業秘密として管理すべき情報資産が大量にあり、各情報資産の秘密性(機密性)のレベルに応じて異なる管理水準による管理体制を構築・実施することが可能である場合には、自社の情報資産を情報の秘密性のレベルに応じて区分し、区分ごとの管理水準・管理方法を設定することが望ましい。

具体的には、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」に分類される情報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については「秘」に分類されることが多い。事業者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。仮に、あまりに多すぎる情報について、これらの指定を行って厳しく管理しようとする、管理のコストが増大したり、管理の実効性確保が困難になったりすることもある。

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。加えて、「極秘」「厳秘」情報の相対的価値が低下することになる。

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。

取引先等の他社から開示された情報については、それが記録されるなどした媒体に当該他社の区分が付されていることが想定される。その媒体を返還する義務がない場合やその複製の作成を許されている場合には、他社との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。

なお、情報の区分・秘密情報の指定の時には秘密情報であったものが、その後公知情報となることがあるため、定期的に又は必要に応じて、情報の区分・秘密情報の指定について見直しを行うことも考えられる。

アクセス権者の指定

営業秘密ごとにアクセスできる権限をもつ者をあらかじめ指定する。
営業秘密へのアクセス記録を残す。

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」をあらかじめ指定しておく必要がある。この場合、従業者の氏名といった固有名詞による特定に限らず、部門の長の許可を受けた部員のみというような方法も考えられる。

秘密性のレベルに応じて営業秘密を区分・指定している場合には、その営業秘密を必要な者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、秘密性のレベルに応じてアクセス権者の範囲は異なり、秘密性の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。

< 一般的な管理方法 >

(秘密の指定)

営業秘密管理規程等の文書によって営業秘密として管理すべき情報を指定し、従業者等に周知する。

他社の秘密情報については、そのことが客観的に分かるように管理すべき情報として指定し、従業者等に周知する。

(アクセス権者の指定)

営業秘密にアクセスできる者(アクセス権者)を、その氏名等により文書等で指定する。

営業秘密にアクセスできる者(アクセス権者)を、役職、特定の部署の配属者、特定の事業の担当者、部門の長の許可を受けた部員等により文書等で指定する。

< 高度な管理方法 >

(秘密指定、アクセス権者の指定)

- ・ 情報の秘密性のレベルに応じて区分し、区分ごとの管理水準・管理方法を設定する。
- ・ 秘密性の区分に応じ、アクセス権者を役職等により範囲を限定して指定する。
- ・ アクセス権者の役職等に応じ、同じ秘密性の区分の営業秘密について、許される取扱方法を区分する。

(他者の営業秘密を不正取得していないことを証明するための措置)

- ・ 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)を実施する。
- ・ 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)を実施する。

< 裁判例 >

「アクセス制限」については、事業者の規模・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員の人数等を限定していることが、秘密管理性を判断する際に肯定的な要素となることを判示しているものがある。

- ・ 書類の管理責任者が総務事務担当 2 名に限定されており、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²⁷
- ・ 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 名の従業員に限定していた例²⁸
- ・ 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、出力の操作手続を知る者を 3 名のみとしていた例²⁹

なお、秘密管理性を認めなかった裁判例の中には、書式等の収められたフロッピーディスクについて、当該フロッピーディスクを取り扱うことができる社員を限定するなどの特段のアクセス制限措置が採られていなかった例³⁰、顧客情報が記載された情報カードについて、一般顧客からは見えない店舗の受付カウンター（レジ台）の棚に備え置かれているものの、その扉は常時施錠されているわけではなく、閉められていないことも多かったという場合において、アクセス制限の存在が否定された例³¹等がある。

²⁷ 前掲大阪高裁平成 14 年 10 月 11 日判決

²⁸ 前掲東京地裁平成 16 年 5 月 14 日判決

²⁹ 前掲東京地裁平成 11 年 7 月 23 日判決

³⁰ 前掲東京地裁平成 12 年 9 月 28 日判決

³¹ 東京地判平成 16 年 9 月 30 日判決

(2) 物理的・技術的管理³²
基本的な考え方

営業秘密が記載・記録されている書面、記録媒体(USB メモリなど)等の管理に当たっては、媒体、保管庫、保管施設等について、媒体に記載・記録されている情報が秘密であることを認識できる措置を講じ、かつ、権限のない者がその媒体(又は情報)にアクセスすることができない措置を講じることが重要である。

営業秘密として管理すべき情報のうち、紙や USB メモリなどの記録媒体(有体物)により保存されているものに関しては、媒体に秘密である旨を表示したり、分離保管したりすることが重要である〔秘密表示、分離保管〕。また、営業秘密が記録されている記録媒体等にアクセスできる者がこれを適切に保管するために、持出し・複製の制限を行い、廃棄の際には復元不可能な形にする〔媒体の保管、持出し、複製の制限と廃棄〕ことが非常に有効である。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こと〔施設等の管理〕等によって管理することも非常に有効である。

物理的管理

(ア) 秘密表示、分離保管

営業秘密が記載・記録されている媒体であることを、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にする。

具体的には、書面にマル秘マークを押したり、電子ファイルの開封に関するパスワードを設定したり、記録媒体などを他の情報のみが記録されているものと分離して保管したりすることなどが考えられる。

(a) 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、営業秘密が記載・記録されている媒体に秘密であることを示すことが考えられる。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。

例えば、紙媒体に記載されている情報であれば、スタンプを押したり、シールを貼付したりすることなどが考えられる。

また、電子情報の場合は、紙媒体と同様に、電子情報を記録している USB メモリなどの記録媒体にシールを貼付することが考えられるほか、電子情報の性質上、営業秘密であること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や、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。

³² 「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.jp/dec/doc/JIP-ISMS100-20.pdf>) 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」等に相当するものである。

(b) 媒体の分離保管

営業秘密が記載・記録されている媒体を、その他の情報が記載・記録されている媒体と分離して保管することが考えられる。

また、電子情報の場合は、上記秘密表示・分離保管に代わって(又は併せて)、電子情報を記録しているファイルなどにパスワードを設定したり、ファイルなどを暗号化したりすることが考えられる。

(c) 営業秘密の表示と分離保管の関係

営業秘密の表示と分離保管は、これを併せて行くと非常に有効であるが、営業秘密が記載されている全ての書面に秘密表示をしたり、同様の記録媒体のみを分離して保管したりすることが過大な負担といえる場合もある。

もとより、営業秘密の管理のための具体的な管理方法は、いずれもその措置を講じないことをもって直ちに合理的な秘密管理とはいえないものではないが、営業秘密の表示又は分離保管については、いずれか一方の措置を講じることによっても、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することができるために相当に有効な措置であると考えられる。

< 一般的な管理方法 >

(秘密の表示 - 全般)

営業秘密が記載されている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・マークなどを記載・記述する。

(秘密の表示 - 紙媒体)

紙媒体に「極秘」や「秘」等のスタンプを押す。

紙媒体に「極秘」や「秘」等のシールを貼付する。

(秘密の表示 - 記録媒体)

記録媒体に「極秘」や「秘」等のシールを貼付する。

営業秘密であることを表示するデータを電子情報そのものの中に組み込む。

電子情報を記録しているファイルの開封に関するパスワードを設定する。

(分離保管)

保管室や保管庫の中に営業秘密が記載・記録されている媒体専用のスペースを設ける。

営業秘密が記載・記録されている媒体専用のファイルなどに保管する。

< 高度な管理方法 >

(秘密の表示)

- ・ プリンターでデジタル透かし情報（廃棄期限や秘密表示等）を付加する。
- ・ 営業秘密であることに加え、どの秘密性のレベルかを表示するデータをも電子情報そのものの中に組み込む。
- ・ 電子情報を記録しているファイルの開封に関するパスワードの設定に関し、秘密性（機密性）のレベルに応じて設定する。
- ・ 電子情報を記録しているファイルを暗号化する。

(分離保管)

- ・ 営業秘密が記載・記録されている媒体を専用の保管庫に保管する。

< 裁判例 >

「秘密表示、分離保管」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が存在すること、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ことが、秘密管理性を判断する際に肯定的な要素となることを判示しているものがある。

(秘密の表示)

- ・ 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³³

(分離保管)

- ・ 印字された顧客名簿を、施錠されている保管室に保管している例³⁴

なお、秘密管理性を認めなかった裁判例の中には、営業秘密の侵害時には特段機密事項である旨の表示が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、単に本件情報が極めて重要であり、性質上「機密」に該当するというだけでは足りず、原告が現実的に、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³⁵、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³⁶、図面の端にドイツ語及び英語で小さく秘密である旨が表示されていた場合において、そうした記載のみをもって、

³³ 前掲東京地裁平成 17 年 6 月 27 日判決

³⁴ 前掲東京地裁平成 11 年 7 月 23 日判決

³⁵ 大阪地裁平成 12 年 7 月 25 日判決

³⁶ 前掲大阪高裁平成 17 年 2 月 17 日判決

従業者らにおいて当該文書が機密文書である旨が明確に認識できるようにしてあったものとは言い難いとした例³⁷等がある。

(イ) 媒体の保管、持ち出し、複製の制限、廃棄

営業秘密を記載・記録している媒体は、保管庫に施錠して保管する。
上記媒体については、その持ち出しをできる限り制限する。
上記媒体の複製についてもできる限り制限する。
上記媒体は、適切に回収する。
上記媒体は、復元不可能な措置を講じて廃棄する。

(a) 保管

書類又は USB メモリなど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に施錠して保管する。

なお、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のが望ましい。

(b) 持ち出し・複製の制限

アクセス権者による媒体の持ち出しや複製を認める場合には、その点に関するルールを設け、できる限り制限することが望ましい。

(c) 回収・廃棄

一時的な説明、使用等のために配布した紙等については、用済み後、直ちに回収するなどの措置を講じることが望ましい。

また、情報が記録された媒体を廃棄する場合は、複製記録や送信記録等の保存を行った上で、復元不可能な形にして行うことが望ましい。

< 一般的な管理方法 >

(保管)

施錠可能な保管庫（金庫、キャビネットなど）に施錠して保管する。

実際に施錠管理をしていることが必要（利用時のみ又は業務時間のみ開錠するなど）であって、施錠できる保管庫であっても常に開錠している場合は適切とはいえない。

(持ち出し・複製の制限)

媒体の持ち出しや複写、複製を一律に禁止する。

アクセス権者による媒体の持ち出しを認める場合には、責任者の許可を必要と

³⁷ 東京地裁平成 19 年 12 月 26 日判決

する。

アクセス権者による媒体の持ち出しを認める場合には、持出の期間や場所の制限（自宅への持ち帰りの禁止等）を行う。

アクセス権者による媒体の持ち出しを認める場合には、施錠付きの鞆等に入れてその者自らが携行し、手元から離さないこととする。

複写を認める場合には、責任者の許可を必要とする。

（回収・廃棄）

営業秘密が記載された資料は配布後、適切に回収する。

営業秘密が記載・記録された媒体が不要となったときは、適宜又は定期的に廃棄する。

< 高度な管理方法 >

（持ち出し）

【記録媒体（可搬記録媒体〔USBメモリ、マイクロディスクなど〕やノートパソコンの持ち出しにより、これに記録された営業秘密を持ち出す必要がある場合）】

- ・ 暗号化機能（ハードウェア実装が望ましい）や生体認証機能（指紋認証、顔認証、静脈認証等）等の機能を有した可搬記録媒体やノートパソコンを利用する。
- ・ 遠隔操作によるデータ消去機能を有するノートパソコンを利用する。
- ・ 記録媒体に含まれる情報全体を暗号化するソフトウェアを利用して暗号化する。
- ・ 記録媒体に情報を記録せず、外部から自社のサーバーに直接アクセスする（ただし、社内でのアクセス制限と同様の、人的・物理的・技術的管理が必要。）

（複製）

- ・ 書類について、コピー偽造防止用紙（コピーできないものや浮き出し文字によって不正コピーであることを明らかにするものなどがある。）を使用する。
- ・ 電子情報を書類に印字出力するに際し、ICカードと複合機とを連動させることによって、利用者制限、枚数管理等を実施する。
- ・（サーバー上のデータをクライアント端末に保存することを防ぐため）パソコンをシンクライアント³⁸化する。

（廃棄）

- ・ 専門処理業者に依頼して溶解処分をする。
- ・ シュレッダーにより書類を廃棄処理する際、書類に付加されたデジタル透かし

³⁸ クライアント側のコンピュータのうち、最低限の機能のみを有するものを指し、サーバーがアプリケーションソフトやデータなどを管理すること。

情報を確認し、廃棄期限が到達しているもので廃棄されていないものがないか確認する（デジタル透かし情報について定期的にリーダーによる読み取り検査を実施することも考えられる。）

- ・ 記録媒体について、消去用ソフト、磁気消去等により記録された情報を消去した後、物理的に破壊する。

< 裁判例 >

「媒体の保管、廃棄」に関しては、（実際に）鍵のかかった引き出しに保管されていること、専門業者に焼却依頼をしていることなどが、秘密管理性を判断する際に肯定的な要素となることを判示しているものがある。

- ・ 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³⁹
- ・ 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⁴⁰

なお、秘密管理性を認めなかった裁判例の中には、顧客情報が記載された見積書について、営業担当者がその控えを保管し、その保管方法は各自に委ねられていた例⁴¹等がある。

（ウ） 施設等の管理

営業秘密の保管場所を施錠する。
営業秘密を保管している施設への入退出を制限する。

営業秘密を保管する場所のセキュリティ配慮については、対象となる営業秘密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重要である。

また、取引先から開示された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には、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施設管理することにより、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。

³⁹ 前掲東京地裁平成 11 年 7 月 23 日判決

⁴⁰ 前掲東京地裁平成 16 年 5 月 14 日判決

⁴¹ 東京地裁平成 19 年 5 月 31 日判決

< 一般的な管理方法 >

(保管場所の施錠等)

- 秘密が保管されている場所を施錠する。
- 業務時間外には警備員を配置する。
- 警備システムを導入する。

(保管場所の区分・入退室管理)

- 秘密が保管されている場所をその他の場所と区切る。
- 「関係者以外立入禁止」等の表示を設置する。
- 営業秘密を管理している施設への入退を制限(ゾーニング)する。
- 営業秘密を管理している施設への入退出の記録を作成する。

< 高度な管理方法 >

(保管場所の区分・入退室管理)

- ・ 保管施設に入退出する際の認証システムとして、IC カード認証、生体認証(指紋認証、こう彩認証、静脈認証等) ワンタイムパスワード(時刻同期方式、イベント同期方式、チャレンジレスポンス方式等)を利用する。
- ・ 上記認証システムに加え、PIN 入力を付与する。
- ・ 保管施設に入退出する際の認証システムとして、アンチパスバック機能⁴²を採用する。

(取引先の秘密情報とのコンタミネーションの防止)

- ・ 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。

< 裁判例 >

「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などが、秘密管理性を判断する際に肯定的な要素となることを判示しているものがある。

- ・ 事務所内に外部の者が訪れた場合には、受付において対応し、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⁴³

⁴² 入室していない ID では退室できず、退室していない ID では入室できない等、同じ ID で続けて入退室できないようにする機能。

⁴³ 前掲大阪高裁平成 14 年 10 月 11 日判決

- ・ 倉庫兼コンピュータ管理室の鍵を、一般の従業員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⁴⁴

なお、秘密管理性を認めなかった裁判例の中には、顧客情報を記した台帳が施錠できる事務所に置かれ、第三者が事務所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⁴⁵、営業秘密であるサービスマニュアルが記載された紙媒体について、当該紙媒体が保管されていた部屋に委託元企業の社員や外注先の業者の従業員が自由に出入りすることができ、これを閲覧しようと思えばすることができたという例⁴⁶等がある。

なお、(ア)~(ウ)の全てについて、責任者を明確にして組織的に行うことが望ましい(「3. 営業秘密の管理を適切に機能させるために実施することが望ましい組織的管理の在り方」を参照)。

⁴⁴ 前掲東京地裁平成 16 年 5 月 14 日判決

⁴⁵ 大阪地裁平成 16 年 5 月 20 日判決

⁴⁶ 東京地裁平成 19 年 6 月 29 日判決

技術的管理

電磁的に記録されているデータの取扱いに関する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。

指定されたアクセス権者にのみアクセス可能な措置を講じる。

営業秘密を保存する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など不正アクセスに対する措置を講じる。

営業秘密のデータを復元不可能な措置を講じて消去・廃棄する。

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、インターネットなど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という観点が必要であり、そのためには、アクセス権者の特定、外部からの不正アクセスなどによる侵入に対する防御等が重要な要素となる。

(ア) マニュアルなどの設定

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 物理的管理と同様であるが、インターネットなどのコンピュータ・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。

(イ) アクセス及びその管理者の特定・限定

営業秘密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など、機密性のレベルに応じた様々な管理が可能である。

また、コンピュータやファイル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、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高い秘密管理性を保つことが可能となる。

なお、ユーザーID 及び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る。

(ウ) 外部からの侵入に対する防御

営業秘密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、営業秘密の盗み見等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重要である。

また、ウイルス感染によるネットワークを通じた情報漏えいを防止するため、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えいを防止するため、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をインストールしないなどの対策を講じることも重要である。

(エ) データの消去、廃棄

電磁的に記録された営業秘密を使用・保管していたコンピュータ・サーバーなど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（ハードディスクなど）内に残っている営業秘密が誤って他者に開示されることのないよう、データの復元が不可能な措置を講じて、電磁的記録の消去又は廃棄することが重要である。

< 一般的な管理方法 >

(マニュアルなどの設定)

コンピュータ・ネットワークに接続する際のルールを確立する。
データ複製、バックアップをする際の手順を文書等で明確化する。

(アクセス及びその管理者の特定・限定)

コンピュータの閲覧に関するパスワードを設定する。
パスワードの有効期限を設定する。
同一又は類似パスワードの再利用を制限する。
情報セキュリティの管理者が退職した場合には、管理者パスワードの変更等を行う。
パスワードに加え、ユーザーIDを設定する。

(外部からの不正アクセスなどに対する防御)

営業秘密を保存・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。
ファイアウォールを導入する。
コンピュータにウイルス対策ソフトウェアを導入する。

< 高度な管理方法 >

(アクセス及びその管理者の特定・限定)

- ・ パソコンの起動又はサーバーにアクセスする際の認証システムとして、ICカード認証、生体認証（指紋認証、こう彩認証、静脈認証等）、ワンタイムパスワード（時刻同期方式、イベント同期方式、チャレンジレスポンス方式）等を利用する。
- ・ 上記認証システムに加え、PIN 入力を付与する。

(外部からの不正アクセスなどに対する防御)

- ・ （外部からの不正なアクセスを監視するため）IDS/IPS を設置する。
- ・ サーバーにアクセスする際の認証システムとして、接続時認証及び通信情報の暗号化措置を講じる。

- ・ 閲覧専用機器もインターネットに接続しない。

< 裁判例 >

「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を定めていることが、「アクセス及びその管理者の特定・限定」については、ユーザーIDとパスワードを設定していることが、「外部からの侵入に対する防御」については、営業秘密を管理するコンピュータを外部と遮断していることが、それぞれ秘密管理性を判断する際に肯定的な要素となることを判示しているものがある。

(マニュアルの設定)

- ・ 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、サーバー・コンピュータ自体の電源を切ることとされていた例⁴⁷

(アクセス及びその管理者の特定・限定)

- ・ 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⁴⁸
- ・ 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、従業員に対し、個別のパスワード（毎月変更する。）を与え、そのパスワードを用いない限り本件顧客情報を取り出すことができないようにした例⁴⁹

(外部からの不正アクセスなどに対する防御)

- ・ 営業秘密を管理するコンピュータは原告代表者のみが使用することができることとされている上、他のコンピュータやインターネットに接続されていない例⁵⁰
- ・ 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ー・コンピュータシステムにより作成、保管されていた例⁵¹

なお、秘密管理性を認めなかった裁判例の中には、各種装置の図面の電子データを必要とする従業員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かった例⁵²、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、事務担当者以外の者も含めて従業員全員がパスワードを知っていた例⁵³、顧客データへのアクセスについては

47 前掲東京地裁平成 16 年 5 月 14 日判決

48 前掲大阪地裁平成 15 年 2 月 27 日判決

49 前掲東京地裁平成 11 年 7 月 23 日判決

50 前掲東京地裁平成 17 年 6 月 27 日判決

51 前掲東京地裁平成 16 年 5 月 14 日判決

52 前掲大阪高裁平成 17 年 2 月 17 日判決

53 東京地裁平成 15 年 5 月 15 日判決

パスワードなどによる保護はされておらず、事務所にいる者なら誰でも見ることができる状態にあった例⁵⁴等がある。

⁵⁴ 東京地裁平成 14 年 4 月 23 日判決

(3) 人的管理⁵⁵ 基本的な考え方

厳重な物理的・技術的管理方法を採用しても、それを遵守すべき者が秘密管理の重要性を理解していなかったり、採用されている管理方法を的確に認識していなかったりした場合には、実効的な管理がなされず、その結果、意図的か否かにかかわらず、営業秘密が漏えいする危険性が相当にあるといえる。

そこで、アクセス権者であるか否かにかかわらず、全ての従業員等において、自社の秘密保護に関する認識を持ち、営業秘密侵害や漏えいを防止するような意識を持つことが重要である。

そのため、事業者としては誰がどのような営業秘密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とともに、自社における営業秘密の取扱いに関するルール等を周知徹底させるために、日常的に教育・研修等を行う。

また、従業員、退職者、派遣従業員、転入者、取引先等、対象に応じた適切な管理を行う。

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、アクセス権者が秘密管理の重要性を理解していなかったり、採用されている管理方法を的確に認識していなかったりした場合には、厳重な物理的・技術的管理方法を採用したとしても、実効的な管理がなされず、その結果、意図的か否かにかかわらず、営業秘密が漏えいする危険性が相当にあるといえる。そこで、アクセス権者が営業秘密として管理すべき情報を秘密として適切に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が重要であることはもちろん、これに加えて、アクセス権者以外の者も含め全ての従業員等において、自社の秘密保護に関する認識を持ち、営業秘密侵害や漏えいを防止するような意識を持っていることが重要である⁵⁶。

アクセス権者については、事業者としては誰がどのような権限・能力を有しているかを把握した上で、誰にどの範囲の営業秘密へのアクセスを認めるかを判断するとともに、当該アクセス権者が負う責務を明確にする必要がある。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、当該事業者における営業秘密の取扱いに関するルールなど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、事業者と従業員等が同じ方向性を持って協力しながら事業者の営業秘密を守っていくことが可能に

⁵⁵ 「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。

⁵⁶ 仮に従業員等が法的な責務を負っているとした場合にも、現実に秘密として管理されているといえなければ、営業秘密性は認められないものと考えられる（大阪地裁平成 11 年 9 月 14 日判決参照）。

なり、それが、最も実効性が高まる方法であるものと考えられる。

また、特に営業秘密の漏えいの主体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、退職者が負う退職後の責務に関して、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。そうした退職後の秘密保持契約等においては、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。

人的管理

(ア) 従業者等に対する教育・研修の実施

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等について、教育・研修を実施する。

アクセス権者に対し、自身が扱う営業秘密の価値及び秘密を保持することの重要性について、よく認識するように教育することが重要である。また、営業秘密管理について組織的な体制を整備していたり、具体的な管理方法を社内ルールとして指定していたりする場合には、アクセス権者であるか否かを問わず、これらについてもよく認識するように、教育・研修を実施することが望ましい。

また、事業者の負担可能な人的コストなどにもよるが、継続的かつ実効的な教育・研修を実施することが理想的であることから、事前に、教育・研修責任者の設置、教育・研修内容の決定をすることが望ましい。

(a) 教育・研修責任者の設置

組織内における教育・研修責任者を事前に定めておくことが考えられる。

教育・研修責任者は組織に属する者に対する定期的な教育等の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、営業秘密管理規程等において教育責任を明確化することが考えられる。

(b) 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・研修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・研修内容を組織内で均一化するために事前に教育・研修内容を定め、場合によって内容に差異が生じないように配慮することが望ましいと考えられる。

(c) 教育・研修の実施

営業秘密にアクセスする者に対して、できる限り定期的な教育・研修を実施することが望ましい。

また、アクセス権限の有無を問わず、営業秘密の管理に関する一般的な教育・普及活動を行う。

さらに、営業秘密を取り扱う頻度が高い従業員等に対しては、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等も含めて教育・研修を実施することが望ましい。

< 一般的な管理方法 >

(教育・研修の実施)

定期的に行われる朝礼等の際に、随時、営業秘密の取扱いに関する注意喚起を行う。

従業員等に対し、秘密管理の重要性について定期的な教育を実施する。

営業秘密にアクセスする者に対し、定期的な教育を実施する。

教育・研修責任者に対し、定期的な実施する教育・研修において、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とさせる。

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実施することが合理的な実施方法の一つであると考えられる。

< 高度な管理方法 >

(教育・研修責任者の設置)

- ・ 営業秘密管理規程等において、「管理責任者は教育責任を負う」など、教育責任を明確化する。

(教育・研修内容の決定)

- ・ 教育・研修内容を組織内で均一化するために、「情報管理の重要性」、「営業秘密の管理組織の概要」、「具体的な管理方法(株式会社 営業秘密管理規程の内容について)」等、教育ツールやカリキュラムを作成する。

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これらのカリキュラムなどを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。

(教育・研修の実施)

- ・ 理解度確認付 e-ラーニングなど全員の受講が確認できる教育プログラムを実施することによって、情報管理の重要性について意識付けする。

< 裁判例 >

「教育・研修の実施」については、これを実施していることが、秘密管理性を判断する際に肯定的な要素となることを判示しているものがある。

- ・ 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⁵⁷
- ・ 就業規則において、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⁵⁸
- ・ 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えい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⁵⁹
- ・ 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⁶⁰

(イ) 就業規則・契約等による従業者、退職者等への秘密保持の要請

契約、誓約書等により、営業秘密を開示した相手方(従業者、退職者等)の秘密保持義務を明確にする。

就業規則や各種規程に秘密保持義務を規定し、従業者等に周知する。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。

退職者に秘密保持義務を課したい場合には、できる限り秘密保持契約を締結する。

(a) 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・就職時の雇用契約に基づき、又はこれに付随して信義則上秘密保持義務を負うが、その内容を就業規則や個別の契約・誓約書等によって明確化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、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、就業規則等において、対象となる営業秘密の範囲は別途指定する旨規定し、従業者ごとに対象範囲を指定する方法等が考えられる。

就業規則による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により直ちに失われるものではないと考えられるものの、退職後に負う秘密保持義務等の範囲を明確化することが望ましいといえること

⁵⁷ 前掲東京地裁平成 12 年 11 月 13 日判決

⁵⁸ 前掲東京地裁平成 16 年 5 月 14 日判決

⁵⁹ 前掲東京地裁平成 14 年 12 月 26 日中間判決

⁶⁰ 前掲東京地裁平成 17 年 6 月 27 日判決

から、退職時に役員・従業者との間で秘密保持誓約書等を交わすことが重要である。

(就業規則において秘密保持の規定を設けるときの留意点等)

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又は使用若しくは開示した従業者に対する制裁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法的規範としての性質を有するものとして、拘束力を生じるためには、事業場の労働者に対して周知されていることなども必要である⁶¹。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。さらに、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。

また、就業規則等に秘密保持義務の規定を設けた場合であっても、公益通報者保護法に基づく公益通報等が妨げられないことは当然であり、事業者においては、その実情に応じて、別途その旨の注意喚起を図ることも考えられる。

なお、事業者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。

(b) 従業者等、退職者等と締結する契約等

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、又はこれに付随して信義則上秘密保持義務を負うが、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。

また、退職者に対して秘密保持義務を課す場合には、できる限り秘密保持契約を締結することが望ましい。

現職の役員・従業者又は退職者と秘密保持契約等を締結する際には、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。

⁶¹ 最高裁平成 15 年 10 月 10 日判決

【従業者、退職者等との間の秘密保持契約等の内容】

秘密保持契約(誓約書を含む。)に盛り込む内容については、例えば 対象となる情報の範囲、秘密保持義務及び付随義務、例外規定、秘密保持期間、義務違反の際の措置等が挙げられる。

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。

・ 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。

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得る。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る。

また、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() ()及び()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えいのリスクなどに配慮して具体化が難しい場合は、下記の() ()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えい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などの対応をとることが望ましい。

() 概括的な概念による特定

「～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。

() 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、「ラポノート 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。

この方法は、()の形式による特定方法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規定とすることが可能である。

() 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¹の飽和脂肪酸含量が ~ 重量%であり、炭素数 以上²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。

・ 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も考えられる。

- 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

・ 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などのやむを得ない場合も、当該開示に限って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や、秘密の開示を最小限度にすることを義務付けること(例えば、開示に際しては、できる限り自社の指示に従うべき旨規定するなど)が考えられる。

- 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など）も存在する。

秘密保持契約において、期限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、元従業員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。

- 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」の中にも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、損害賠償額を予定したりすることはできないことに留意する必要がある。

【秘密保持契約を締結するタイミングと事務手続】

秘密保持契約を締結するタイミングとしては、入社時、在職中（特定のプロジェクトへの参画時等）、退社時、があるが、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、在職中、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を各事業者が考え、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。

- 入社時

職種を限定して採用した従業員については、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ため、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。

- ・ 在職中(特定のプロジェクトへの参画時等)

事業者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。

なお、プロジェクト終了後においては、秘密保持義務の対象となる情報が記録等された媒体を会社に返還させるとともに、従業員自らが保有するパソコンやUSBメモリなどに秘密保持義務の対象となる情報が記録等されている場合においては、当該情報を消去した上で、当該消去した旨を会社に報告させるなどの対応を行うことも考えられる。

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。また、退職時までの期間がより短くなっていることから、当該従業員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。

- ・ 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、各種プロジェクトなど、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がされると、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、一定期間ごと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後、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。

(c) 退職者との競業禁止契約

秘密保持に関して、退職後の従業者等に対して競業禁止義務を課すことも考えられる。しかしながら、競業禁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、競業禁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（競業禁止義務の有無は、「秘密管理性」の判断とは別個のものである。）

なお、競業禁止義務については、裁判例上、「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ず、かかる「合理的範囲を確定するにあたっては、制限の期間、場所的範囲、制限の対象となる職種の範囲、代償の有無等について、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）の三つの視点に立って慎重に検討していくことを要する」ものと判示されている⁶²。

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、退職後に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や⁶³、退職後 6 か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⁶⁴等がある。）

< 一般的な管理方法 >

(就業規則等)

就業規則等において秘密保持の規定を設ける。

就業規則等において包括的・一般的な秘密保持の義務規定を設けるに留まる場合には、対象となる営業秘密の範囲は別途指定する旨規定し、従業者ごとに対象範囲を指定する。

⁶² 奈良地裁昭和 45 年 10 月 23 日判決

⁶³ 最高裁昭和 52 年 8 月 9 日判決

⁶⁴ 名古屋高裁平成 2 年 8 月 31 日判決

(従業員、退職者等と締結する契約)

現職の従業員等に対し、個別の契約・誓約書等により秘密保持義務を課す。
退職者との間で、秘密保持契約を締結する。

(退職者との競業避止契約)

退職後の従業員等に対して競業避止契約を締結し、一定期間の競業避止義務を合理的範囲内で課す。

< 裁判例 >

「就業規則等」、「従業員、退職者等と締結する契約」については、これを実施していることが、秘密管理性を判断する際に肯定的な要素となることを判示しているものがある。

- ・ 就業規則において、社員は、会社が指示した秘密事項を自己の担当たと否とを問わず、一切外部に漏らしてはならず、秘密事項を公表しなければならないときは、会社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⁶⁵
- ・ 営業秘密に接する機会のある従業員に対し、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などを記載した誓約書を提出させてきた例⁶⁶
- ・ 秘密事項を知り得る立場にある営業関係の従業員全員に、退職後に秘密事項を漏えいしない旨の誓約書を作成させて秘密保持義務を課していた例⁶⁷

なお、秘密管理性を認めなかった裁判例の中には、就業規則に「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、これは業務上の機密事項に関する従業員の守秘義務を一般的に定めたものにすぎないとした例⁶⁸、就業規則で定めたり、又は誓約書を提出させたりするなどの方法により従業員との間で厳格な秘密保持の約定を定めるなどの措置をとっていないという例⁶⁹、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、ディスクなど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

⁶⁵ 前掲東京地裁平成11年7月23日判決

⁶⁶ 前掲東京地裁平成17年6月27日判決

⁶⁷ 大阪高裁平成20年7月18日判決

⁶⁸ 大阪高裁平成15年1月28日判決

⁶⁹ 東京地裁平成16年4月13日判決

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⁷⁰、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であることができるが、同規定は、原告の備品等を大切に、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⁷¹、などがある。

(ウ) 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程度の秘密保持義務を遵守するよう規定する。
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（受入先の事業者）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。

この場合、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程度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。

⁷⁰ 前掲東京地裁平成 17 年 2 月 25 日判決

⁷¹ 大阪地裁平成 17 年 5 月 24 日判決

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。

< 一般的な管理方法 >

派遣契約において、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義務と同等の秘密保持義務を遵守するよう規定する。

(エ) 転入者

他の会社から転職した者を採用するときには、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。

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。

(a) 転入者の契約関係の確認

採用予定の転入者に対してインタビューなどを行うことで、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する必要がある。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、転入者が退職時に差し入れた誓約書等の写しを退職元企業が転入者に交付しないため、若しくは契約書の内容を開示しない契約を退職元企業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分からない。この場合においても、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、不正競争防止法上の責任が生じ得ることから、「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。

(b) 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（a）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、漏えい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。

(c) 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、退職元企業との間で秘密保持義務違反が生じないように確認をすることが望ましい。また、配属についても、転入者が負う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。

< 一般的な管理方法 >

他社の営業秘密の不正な使用又は開示を前提とした採用活動は行わない。
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する。
転入者の配属について、転入者が転入前の会社に対して負っている競業避止義務や秘密保持義務に留意する。
退職元企業における業務内容・秘密保持義務の内容等、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する。
退職元企業に対して、退職時誓約書の内容等について問い合わせる。
退職元企業から警告書が届いた場合には、その内容につき、当該転入者等に十分に確認する。

(オ) 取引先

取引先に自社の営業秘密を開示する場合には、開示する前に相手方に秘密保持義務(守秘義務)を負わせる内容を含む契約を締結する。

取引先から開示された情報については、自社情報との間で、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。

(a) 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、本契約の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。この点、「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あり得ることから、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、それぞれの事業者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。

(b) 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。

() 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、相手方が当該情報の開示につき正当な権限を有するか否かについて、相当の注意を払う必要がある。

() 取引先への組織的対応

メーカーなどにおいては、新規取引先から新技術・製品の売込みを受けることがしばしばあるが、事業者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、社内に対応を統一する方法も考えられる。

() 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すれ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、契約に基づき取得した場合は、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り得ることに留意する必要がある。

【事業者間の秘密保持契約の内容】

・ 事業者間の秘密保持契約の特徴

事業者間の秘密保持契約においても、基本的に事業者と従業者等・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ことが考えられる。

したがって、秘密保持契約に盛り込む内容については、例えば 対象となる情報の範囲、秘密保持義務及び付随義務、例外規定、秘密保持期間、義務違反の際の措置等⁷²があげられる。

しかしながら、事業者間の秘密保持契約に特有と考えられる事項として、以下の点が挙げられる。

() 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、事業者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などが考えられる。

⁷² 前掲「(イ)就業規則・契約等による従業者、退職者等への秘密保持の要請 (b) 従業者等、退職者等と締結する契約等」の【従業者、退職者等との間の秘密保持契約等の内容】参照。

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。

() 秘密管理体制の構築の要請

当該営業秘密の秘密管理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、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などが挙げられる。

() 契約期間と秘密保持義務の存続期間

事業者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。

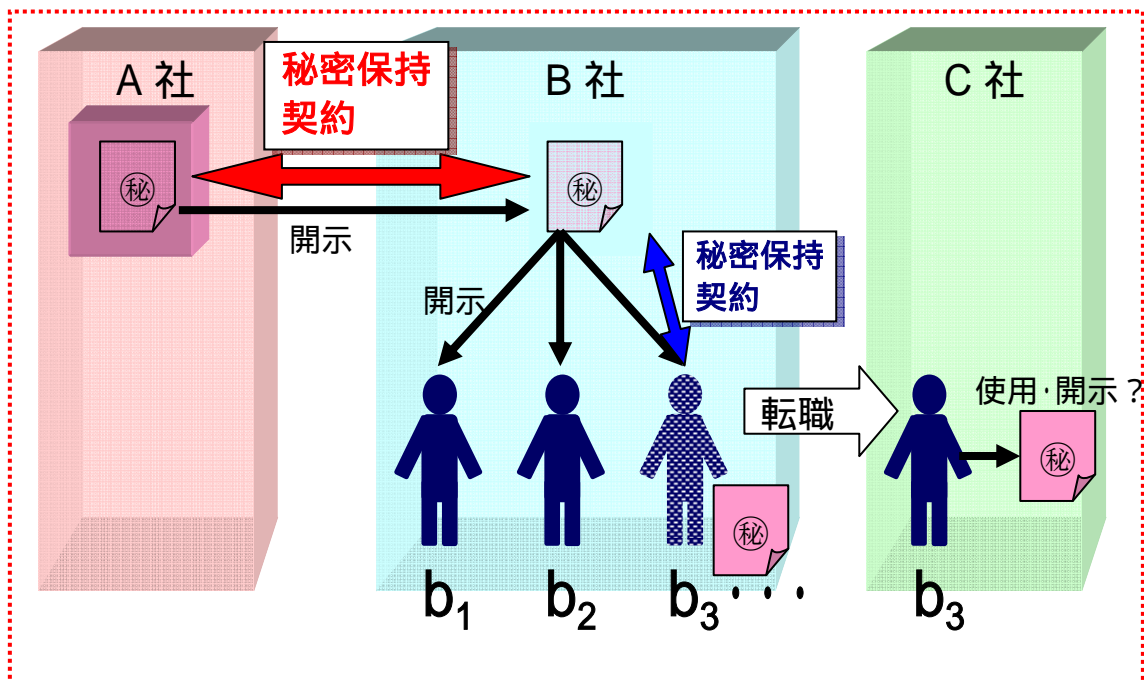
これは、契約期間は、契約に規定された目的を達成するのに必要な期間であり、全ての規定の遵守を求めるものであるのに対し、秘密保持義務の存続期間は、契約条項の中でも、秘密保持義務についてのみ、より長期の存続を求める場合があるからである。

・ 事業者間の秘密保持契約と、事業者と従業者・退職者等との間の秘密保持契約の関係

事業者が従業者等・退職者との関係で締結する秘密保持契約は、事業者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、ライセンス契約に基づいてA社(ライセンサー)の営業秘密をB社(ライセンシー)に開示するケース(次図参照)では、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とが考えられる。この場合、B社において開示を受けた営業秘密を実際に使用するのは、B社の従業者b₁、b₂、b₃...であるが、B社がb₃との間で秘密保持契約を締結することなく、b₃がC社に転職した場合には、b₃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り、その結果、B社は適切な秘密管理体制を構築しなかったとしてA社に対して損害賠償の責を負う場合があり得る。(次図参照)

言い換えれば、事業者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、秘密保持契約において、B社内で開示をする従業者に対しては、B社において秘密保持義務を課すべき旨が定められているなど、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。



< 一般的な管理方法 >

会社間で取引を行う場合には、取引の開始時において、秘密保持の対象となるか否かを明確に定めた秘密保持契約を締結する。

共同開発等の過程で事前の契約等において指定した営業秘密の範囲を超えるものを口頭で開示した場合には、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など、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。

取引先から重要なノウハウなどの開示を受ける場合には、相手方に当該ノウハウの帰属を確認するとともに、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などについて、取引先に表明又は保証してもらう。

(4) 営業秘密侵害に備えた証拠確保等に関する管理

厳重な管理方法を実施した場合であっても、営業秘密が漏えいするおそれを完全になくすことはできない。

そこで、営業秘密が漏えいした場合に備え、証拠確保のための措置を講じることが考えられる。

営業秘密を管理する方法として、情報自体の物理的・技術的管理、取り扱う人の管理等について提示してきたが、どのように厳重な管理方法を実施した場合であっても、営業秘密が漏えいするおそれを完全になくすことはできない。

また、営業秘密が実際に漏えいした場合については、その漏えい経路を明らかにし、侵害者に対して責任追及をするための証拠を確保する必要がある（責任追及を裁判手続において行う場合には、その侵害事実を立証するために適切な証拠が必要となる。）

そのため、営業秘密が実際に漏えいした場合に備え、証拠確保のための措置を講じることが考えられる。また、このような措置を講じることが、意図的に営業秘密を侵害しようとする者に対し、不正行為を思いとどまらせる効果を期待することもできる。

< 管理方法 >

- ・ 営業秘密が記載・記録されている書面、記録媒体等を、閲覧や複製や持ち出しした者を台帳に記録する。
- ・ 営業秘密を取り扱っている従業員等のコンピュータの利用状況や通信の記録を保存する。
- ・ （従業員等が在職中に営業秘密の不正な使用、開示等をした場合、営業秘密の漏えいが発覚するまで時間がかかる場合があるため）営業秘密を取り扱っていた従業員等が退職した場合等には、その使用していたコンピュータのデータを一定期間保存する。
- ・ 営業秘密を管理している施設への入退出の記録を作成する。
- ・ （不正な持ち出しを監視・記録するため）営業秘密を保管している施設に監視カメラを設置し、記録する。
- ・ 営業秘密が記載・記録されている書面、記録媒体等に対して、予めデジタル透かし情報（秘密表示、管理者情報等）を付加する。

3. 営業秘密の管理を適切に機能させるために実施することが望ましい組織的管理の在り方⁷³

(1) 基本的な考え方

営業秘密の管理においては、個別の管理方法を実効的に実施し、発生した問題に的確に対応していくため、組織的な管理を行うことが重要である。その際、自社の営業秘密の管理という視点のほか、他の事業者の営業秘密を侵害しないという視点をももつことが必要である。

営業秘密の管理においては、個別の物理的・技術的・人的管理等の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、組織的な管理を行うことが重要である。すなわち、自社（他の事業者から正当に開示を受けたものを含む。）の営業秘密の漏えいを防ぎ、漏えいの実事又はその危険性を早期に発見し、状況を改善していくためには、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管理を行うことが重要である。

このシステム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等を継続的に行う必要がある。「2. 営業秘密の管理のために講じることが望ましい秘密管理方法」で紹介した具体的管理方法が、このような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。

また、営業秘密について組織的な管理を行う際には、自社の営業秘密を外部に漏えいさせないという視点のほか、自社の従業者等が、他社の営業秘密を不正に取得したり、他社の営業秘密を不正に使用又は開示したりしないという視点も必要である。

以下、(2)において他の事業者の営業秘密を侵害しないという視点をもつことの意義について記載し、(3)において実効的な組織的管理を行う上で目安となる事項及びそのために実施することが望ましい具体的な措置等について記載する。

(2) 他社の営業秘密を侵害しないための組織的管理の意義

法人は、民事的責任を問われることがあり得るとともに、刑事罰の対象ともなりえ、さらに、事業者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、その事業者の評判に大きな影響を与える可能性もある。したがって、事業者としては、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・具体的な措置を講じることが望ましい。

不正競争防止法においては、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。

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

⁷³ 「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。

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、事業者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事業者の評判に大きな影響を与える可能性もある。

したがって、事業者としては、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・具体的な措置を講じることが望ましい。

両罰規定と選任監督義務（刑事罰）

法人も、刑事罰の対象になることがあり得る上、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ため、従業者等による営業秘密侵害を防止する措置を講じる必要がある。

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「注意を尽く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」である旨の判示がなされており⁷⁴、法人には過失が推定されることから、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こととなる。

また、「事業主が違反の防止に必要な措置をすることは、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」という裁判例もあり⁷⁵、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じる必要がある。

相当の注意（民事上の措置）

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、事業者が悪意又は重過失で営業秘密を取得等した場合には、事業者自身による不正競争行為に該当し得るため、従業者等が正当に営業秘密を取得・開示していることにつき、事業者としては相当の注意を払う必要がある。

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（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。

⁷⁴ 前掲最高裁昭和40年3月26日判決

⁷⁵ 高松高裁昭和46年11月9日判決

このように、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、事業者が悪意又は重過失で営業秘密を取得した場合には、事業者自身による不正競争行為に該当し、損害賠償等の責めを負うことになり得るため、従業者等が正当に営業秘密を取得・開示していることにつき、事業者としては相当の注意を払う必要がある。

(3) 望ましい組織的な管理体制の構築の在り方

重要な情報資産（営業秘密として管理すべき情報資産）の把握

事業者が営業秘密の管理を組織的に行う際には、まず、当該事業者にとって「自社の何が重要な情報資産であるか」が明確であることが基本となる。
また、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を判断することが可能となる。

事業者が営業秘密の管理を組織的に行う際には、まず、当該事業者にとって「自社の何が重要な情報資産であるか」が明確であることが基本となる。

営業秘密として管理すべき重要な情報資産を適切に把握して管理する手順としては、自社の強みとなる情報資産を把握し、そこで把握された情報資産の中から営業秘密として管理すべき対象となる情報資産を特定してその管理方法を決定するものや、自社の情報資産全般についてリスク分析を行い、リスクが大きいものからそのリスクを低減するために必要な措置等を講じるものなどがある。

この点、ある情報が営業秘密として管理すべき重要な情報資産であるか否かは事業者ごとに異なるものであり、一概に指摘することはできないが、一般的に営業秘密として管理される情報は以下のように分類することができる。

情報資産分類	情報資産分類に該当する主な情報の例
経営戦略に関する情報資産	経営計画、目標、戦略、新規事業計画、M&A 計画等
顧客に関する情報資産	顧客個人情報、顧客ニーズなど
営業に関する情報資産	販売協力先情報、営業ターゲット情報、セールス・マーケティングノウハウ、仕入価格情報、仕入先情報等
技術(製造含む。)に関する情報資産	共同研究情報、研究者情報、素材情報、図面情報、製造技術情報、技術ノウハウなど
管理(人事・経理等)に関する情報資産	社内システム情報(ID、パスワード)、システム構築情報、セキュリティ情報、従業者個人情報、人事評価データなど
その他の情報資産	上記以外の情報資産

事業者において、適宜の方法により把握した自社の重要な情報資産を、組織的に管理し、かつ、その創出経緯を明確にしていれば、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をすぐに判別することができる。

また、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を判断することが可能となる。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。

目安となる事項

管理の実効性を確保するため、組織的な管理体制を構築する際に目安となる事項としては、以下の六項目が挙げられる。

管理方針等(基本方針、規程等)の整備

責任者の存在とその権限の明確化

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

日常的なモニタリングの実施

内部監査の実施

事後対応体制の整備

前記 のとおり、事業者においては、自社の重要な情報資産を把握し、これを組織的な管理体制の下、適切に管理することによって、自社の営業秘密を保護するとともに、他社の営業秘密を侵害しないために自社の情報と他社の情報とをしゅん別することができるような取組を行うことが重要であり、そのために実効的な管理体制を構築することが望ましい。

望ましい秘密管理体制の構築をするための目安となる事項としては、以下の六項目が挙げられる。

< 目安となる六項目 >

(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、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、手続を従業員に周知徹底することが重要である。

ただし、教育・研修は、全従業員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のが望まれる。

また、事業者側から見た営業秘密保護の観点だけでなく、従業員保護の観点から、従業員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、従業員への教育・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、その内容を従業員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、また上司の指示等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等に対する措置、更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。

上記六つの項目は、自社の従業者等が他者の営業秘密を侵害した場合に、自社が免責される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い。他方で、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」といえるような実効的手段がと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、営業秘密の組織的な管理に取り組むに際し、従業者全ての行動や社内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、自社の重要な情報資産として把握した情報（群）ごとに、そ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などを勘案し、個々の事業者の経営判断によって必要な措置を講じることが求められる。

望ましい組織的管理のポイント（PDCAサイクルの確立）

実効的な管理体制を構築するためには、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。

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、適切に管理を行うため、前記の目安となる事項を踏まえつつ、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、事業者が、これら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、事業者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。

（ア） 管理方針等（基本方針、規程、基準等）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。

（a） 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、全従業員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、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。

（b） 実施計画の策定

基本方針のみでは、必ずしも具体的な営業秘密管理の手順が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、営業秘密として管理すべき重要な情報資産を適切に把握することが重要である。

この点、前記 にみたように、「自社の強みとなる情報資産の把握」によって営業秘密として管理すべき情報を特定する方法と、「リスク分析」によって営業秘密として管理すべき情報（及び管理）を特定する方法等がある。

まず、「自社の強みとなる情報資産の把握」について説明する。

これを具体的に行う方法については、様々な方法が考えられるが、これまで意識的に営業秘密を含む重要な情報資産の保護に取り組んでこなかった事業者においては、その競争優位を実現させている要素に着目した方法が比較的取り組みやすいと考えられる。そして、この取組の際には、業務プロセスごとに、自社の利益獲得等に貢献している要素（例えば、新規事業計画、顧客ニーズ情報、仕入価格、素材情報、製造ノウハウなどが挙げられる。）を、他社との比較優位性・独自性（特異性）の有無等の観点から分析し、把握することが考えられる。このようにして把握した「自社の強みとなる情報資産」においては、特許権等の排他的な権利を取得するために出願・公開するか、自社の企業評価等を向上させるために広報等により公開するか、自社の優位性を持続させるために秘密として管理するかなどを判断し、営業秘密として管理すべき情報資産を特定することとなる。また、「自社の強みとなる情報資産」の把握方法としては、前記 に記載した表のような情報資産のカテゴリー（概括的な分類・区分）ごとに自社の情報資産の有無・数量・存在形態等を洗い出して把握する方法も考えられる。

なお、自社の強みとなる情報資産の把握によっては、秘密として管理すべき情報資産とされなかった情報であっても、法令上保護することが求められているもの（例えば、個人情報の保護に関する法律に定められた個人情報）や、社外に流出した場合に自社に財産上又は信用上大きな損害を与えることが想定されるもの（例えば、他社から秘密保持契約に基づき開示された情報）は、秘密として管理するべきである。

次に、リスク分析による方法をとる場合には、営業秘密の管理に関するリスク（例えば、コンピュータウイルス、不正アクセスなどの外部要因や対策の不

備、ソフトウェアの故障、人為的ミスなどの内部要因)を洗い出した上で(情報資産管理台帳を作成することなども考えられる。)リスクが顕在化した場合に自社に与える影響の大小(例えば、「事業や経営に深刻な影響を及ぼす」、「業務が停止する」、「業務効率が低下する」など)またリスクが実際の問題にまで発展する可能性・頻度の程度、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、どのような方法によって営業秘密として管理すべき情報資産を把握する場合であっても、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、しかも長期的には営業秘密の管理に関するリスク全体を軽減していくものとして策定することが望ましいと考えられる。

その上で、管理目的はできる限り明確に定め、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る。

(c) 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など)などの社内ルールを設け、従業員等に周知徹底を図るとともに、具体的な営業秘密の取扱方法等を明示することが重要である。

(d) 各種規程類の文書化

上記(a)～(c)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、情報セキュリティポリシーの一部を構成する形で文書化することも考えられる。

(イ) 実施(責任者の設置、従業員への周知徹底) <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、従業員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。

(a) 責任者の存在とその権限の明確化

上記の管理方針等にのっとり、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、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。

() 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、「() 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。

() 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、その性格から次の二つに区分される。事業者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、又は、他社から当該情報を開示され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、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

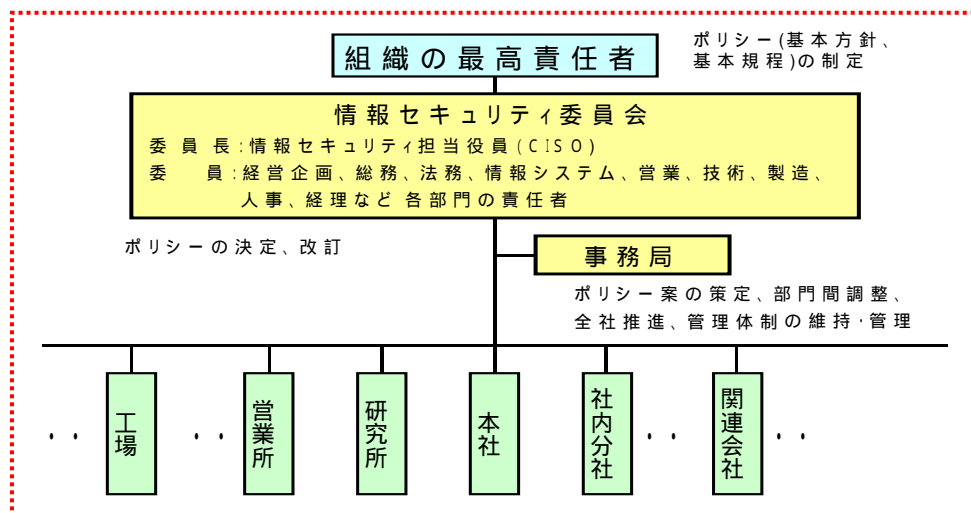
セキュリティの三要素、すなわち、機密性、完全性 (保全性) 、可用性のすべてを確保する責任である。言い換えれば、営業秘密について、正式に許可された者だけが、正しい内容の情報を、必要なときにはいつでも利用

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。

() 望ましい組織体制の例

() () 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。事務局には社内の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。事務局を二つに分割して、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。



(b) 責務の着実な実施

物理的・技術的な管理及び人的管理等を、それぞれの任にある者が着実に実施し、責任者がそれぞれのレベルで、その状況を管理する(前記(a))。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、(c)の教育を行う。

また、他社の情報については、当該従業員の日常的な情報収集活動等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い。

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。

(c) 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など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、事業者側からみ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。

(d) 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。

(ウ) 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、できる限り定期的に内部監査(第一者監査)を実施する。

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などについて、まずは日常的にモニタリングし、その状況を踏まえ、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できる限り定期的に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事業者自身又は代理人によって行われる監査のことである。

監査に当たっては、あらかじめ監査責任者を設置するなど、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を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。

さらに、監査の透明性確保が必要な場合等、内部監査だけでは適切な対応が難しいケースには外部監査を実施する方法もあるが、事業者の規模等から導入が困難な場合も考えられ、必要に応じて導入することが重要である。外部監査には第三者監査と第三者監査がある。第三者監査は、その組織の利害関係者（顧客等）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。

なお、監査の結果を記録として一定期間保存することは、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ことから望ましいと考えられる。

（エ） 見直し< Act >

できる限り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。

（a） 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には、その問題点が、管理方針等自体にあるのか、それとも管理方針等が適切に実施・運用されていないことにあるのかを判断し、仮に管理方針等に問題があ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。

（b） 管理方針等の見直し

監査結果等を踏まえ、従業員の負担の軽減、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、その実効性を確保す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。

< 組織的管理における具体的な措置等 >

管理方針等（基本方針、基準、規程等）の策定 Plan

（基本方針の策定）

「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」の各事項を含む基本方針を策定する。

他社の営業秘密侵害を防止する観点から、基本方針に含むことが望ましい事項

【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
- ・ 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
- ・ 侵害を行った従業員に対する懲戒・刑事告発等を行うための社内手続
- ・ 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

（実施計画の策定）

「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」の各事項を実施計画に含む。

（ルールの構築（社内における開示・公表ルール））

社外に営業秘密を開示する際には（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、社内稟議システムなどの社内手続において開示判断の権限を与えられた適切な者の承認を必要とする。

情報管理規程等、マスコミや学術誌への発表又は取材対応に関する公表ルールを作成する。

インサイダー取引規制関係等の公表ルールがある場合は、調整が必要である。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、対外的な発表は広報室を通して行うなど、情報を一元的に管理する。（広報・IR組織の設置・活用。）

実施（責任者の設置、従業員への周知徹底） Do

（責任者の存在とその権限の明確化）

営業秘密を含む自社・他社情報の取扱責任者を設定する。

段階ごとに（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。

上記組織体制を整備するに当たり、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。

（責務の着実な実施）

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員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（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が発見した場合、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等）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。

他社の営業秘密を取得する可能性が高いケースごとの具体例

【共同開発時】

- ・ 共同開発に際し、他社から営業秘密の開示を受ける場合（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な使用又は開示を行うことがないように配慮する。
- ・ 口頭で情報の提供を受けた場合には、トラブルを未然に回避するため、事後に文書等で営業秘密に該当する情報の確認を行う。
- ・ 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、事業者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、他社従業員からの積極的な売り込みを受け入れたりしない。
- ・ 不正をほのめかすような者の雇入れを避ける。
このような者は、次の就職の際に同じ行動をとる可能性も考えられる。

- ・ 競合他社の従業者であった者を採用する場合に、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⁷⁶】

金型図面等の授受については、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授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等も存在する。

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授受した側が、後に何らかの責任を問われることがないように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などが含まれている場合が多いため、ノウハウなどの帰属については、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、相手側のノウハウなどを知り得る場合には、当該ノウハウなどに関して、秘密保持契約を締結する。

（周知徹底、教育）

【一般従業者に対する周知徹底、教育】

イントラネットなどを通じた法律、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。

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。

「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する。

従業者が非常に不利益を被る競業禁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や担当管理職等に対する教育】

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、担当管理職等については、その立場等に応じた更なる教育・研修活動を実施する。

⁷⁶ 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。

【担当取締役等の情報の取扱責任者に対する教育】

担当取締役等の情報の取扱責任者に対する教育専門家等のサポートを受け、法律及び情報管理方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。

(リスク顕在化への対応)

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。

管理状況のチェック（監査、モニタリング） Check

(日常的なモニタリングの実施)

総括責任者において、各責任者の任務の実施状況に関して、チェックする。

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をする。

社内における周知状況に関する調査をし、不足している場合にはその対応策を検討する。

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を整理する。

(内部監査の実施)

仕事の性質上、営業秘密の漏えい、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、実施する監査手続のレベルを高める、監査頻度を高めるなど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。

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、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。

監査の結果、改善が必要と判断される場合、監査責任者は、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、改善を促す。

「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」より緊急性が低い改善項目に対してなされる。

(監査結果の記録)

監査の結果を記録として一定期間保存する。

見直し Act

管理方針等に問題がある場合には、適切かつ柔軟に見直していく。
組織の経営層によって見直しの内容を実施又は承認する。

(4) 営業秘密の管理と情報管理に関する国際規格(マネジメント規格)、個人情報保護等との関係

現在、事業者等の組織において情報管理をするための適切な仕組み(情報セキュリティマネジメントシステム(ISMS))を構築する際の国際標準として、ISO/IEC27001:2005が位置づけられており、それに基づく第三者認証制度として、(財)日本情報処理開発協会が運用する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事実上の国内標準の地位を占めている。この制度は、営業秘密の管理とのかかわりとしては、これまで述べてきた営業秘密を適切に管理するための具体的な方法を同制度で定める内容に取り込むことにより、営業秘密の要件である秘密管理性が肯定される可能性を非常に高いものとし、情報の漏えいリスクを相当程度低減することができるものとして参考になるものと考えられる。

また、個人情報の保護に関する法律により、個人情報取扱事業者は、その取り扱う顧客情報等の個人情報について、厳格な管理を行うことが求められている。営業活動上の有益な顧客名簿については、このような厳格な管理によって秘密管理性を満たすことにより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などとも整合性をもって秘密管理を行うことが重要である。

このように、事業者の保有する情報の管理に関しては、その流出防止や取扱いに関する法令遵守等、法令上の位置づけの相違に応じた目的等に基づき各種のガイドラインや指針が策定・公表されていることから、事業者においては、これら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、情報の種類ごとに新たな管理体制を構築することなく、組織的な管理が可能となり、あわせて管理コストの低減につながるものと考えられる。

なお、事業者における参考のため、各種ガイドラインなどについて、「参考資料3 我が国における情報管理に関する各種ガイドライン等について」としてまとめている。

営業秘密管理指針

発 行 2003年 1月30日

2005年10月12日 改訂

2010年 4月 9日 改訂

編 著 経済産業省経済産業政策局知的財産政策室

〒100-8901 東京都千代田区霞が関1丁目3番1号

TEL: 03-3501-3752 FAX: 03-3501-3580

E-mail: chitekizaisan@meti.go.jp