はしがき

技術ノウハウや顧客リスト等の営業秘密は、企業の重要な経営資源の一つであり、企業がこれを適切に管理し、漏えいを防止することは、その競争力の維持・強化のために不可欠の課題です。また、雇用の流動化やIT技術の進展により、以前に比べ情報の漏えいや不正使用のリスクが高まっている中、平成27年（2015年）不正競争防止法改正により、営業秘密についての民事・刑事両面にわたる保護が大幅に強化され、自社の営業秘密侵害に対する救済を求めやすくなった半面、他社の営業秘密を侵害しないことの重要性が増大しました。

本書は、このように重要度を増した営業秘密の管理について、それぞれ違った観点からかかわり合いをもつ異業種の執筆者らが、それぞれの実務経験と、企業実務家の方々を交えて3回にわたって実施した「企業秘密合同セミナー」での議論の成果を踏まえ、より実務に直結した営業秘密の適切な管理手法を解説することを主眼において執筆したものです。また、本書は、長きにわたって営業秘密管理のすぐれた実務書として利用されてきた長内健先生のご著書『企業秘密防衛の理論と実務――営業秘密を中心として』を受けて、出版させていただくこととなったものです。

本書の**第1章**「営業秘密管理の必須知識」では、まず、「第1　なぜ『営業秘密』を管理するのか」において、営業秘密の法的な意味を確認したうえで、今日の経済社会における営業秘密の重要性を具体的な事例を通じて解説し、「第2　営業秘密保護と不競法」において、不正競争防止法による営業秘密の保護の概要を説明し、「第3　平成27年改正不競法の内容と意義」において、平成27年改正の概要と同改正を踏まえた営業秘密管理の留意点を説明します。

本書の**第2章**「営業秘密の保護に関する不競法と実務」では、民事・刑事の法的手続により営業秘密の保護を図る際のポイントを解説します。

本書の**第3章**「営業秘密管理の実務」では、営業秘密管理を実践するうえで実務上特に留意すべき事項を「4つの基本的な視点」、すなわち、**視点**①：自社の情報が第三者により侵害されたとき、不競法に基づきその適切な保護、回復が図れるようにしておく視点、**視点**②：自社の秘密情報の管理および利用を、より実効的、積極的、組織的に行っていこうとする場合にもつべき視点、**視点**③：自社の企業秘密が漏えいないし流出してしまった場合にもつべき視

点、および、**視点**④：他社の営業秘密の侵害者であると疑われないようにすることや、疑われた場合に不正を行っていないことを証明できるようにしておく視点、の４つに整理したうえで、まず、**視点**①に関し、「第２　経産省ガイドラインと管理体制」において、不競法を所管する経済産業省知的財産政策室が作成した営業秘密管理指針を踏まえたミニマムスタンダードとしての営業秘密管理のあり方を紹介し、次に、**視点**②に関し、「第３　社内における営業秘密管理体制の構築」において、社内における営業秘密管理の実践的な構築方法について詳しく説明しています。そして、「第４　人事・労務面からみた営業秘密管理」において、人事・労務面からみた営業秘密管理、「第５　営業秘密漏えいへの対応・対策」において、営業秘密漏えいが発覚した場合の対応・対策について、実務的な観点から説明を加えました。さらに、**視点**③に関し、「第６　他社からの営業秘密の漏えい防止」において、業務委託先等の他社から自社の営業秘密が漏えいすることの防止策について解説し、そして、最後に、**視点**④に関し、「第７　他社の営業秘密の侵害防止策」において、他社の営業秘密の侵害をいかにして防止するかについて解説しました。

本書が、営業秘密管理やその再構築を検討されていらっしゃる方々の少しでもお役に立てれば嬉しく思います。

最後に、本書の出版にあたっては、民事法研究会の編集部の皆さまに大変お世話になりました。ここに感謝の意を表します。

平成29年２月

服部　誠
小林　誠
岡田大輔
泉　修二

第3章 営業秘密管理の実務

第1 営業秘密管理の４つの視点

第2 経産省ガイドラインと管理体制

第3 社内における営業秘密管理体制の構築

第4 人事・労務面からみた営業秘密管理

第5 営業秘密漏えいへの対応・対策

第6 他社からの営業秘密の漏えい防止

第7 他社の営業秘密の侵害防止策

第1 営業秘密管理の４つの視点

営業秘密管理においては、以下の４つの視点を意識しておくことが重要である。

第１に、自社の情報が第三者（従業員、元従業員を含む）により実際に侵害されたとき、あるいはその疑いが生じたときに、不競法に基づく保護を受けられるようにしておくことである（視点①）。

営業秘密侵害の被害者となる場面において、不競法の民事・刑事上の保護を受けようとする場合には、保護を求める情報が、秘密管理性の要件を具備するなど、同法上の「営業秘密」（不競法２条６項）に該当することが必要である。基本は、秘密表示の徹底、アクセスできる者の制限、それら情報管理に関するルールの整備とその実践にある。

第２に、自社の秘密情報の管理および利用を、より実効的、積極的、組織的に行っていこうとする場合にもつべき視点である（視点②）。

秘密管理体制の構築に要するコストや各担当者の負担、また従業員のプライバシーや退職の自由といった相対峙する利益との調和を図りつつ、自社にとって最適な秘密管理体制を整えることが求められる。さらに下請け先や共同開発の相手方からの情報流出・漏えいリスクについても考慮し、対処しておく必要がある。視点①が、不競法の秘密管理性の要件を満たすための最低限の低コストでの情報管理のあり方を追求しようとする視点であるのに対し、視点②は、より実効的、積極的、組織的に、秘密情報の管理・利用を行っていこうとする視点である。いずれの視点に立つべきかは、企業価値を高めるためにどのような情報管理を行うべきかという観点から選択されるべきものと考えられる。

第３に、自社の企業秘密が漏えいないし流出してしまった場合にどのように対応していくべきかという視点である（視点③）。

視点①と視点②が平時（事前）の対策に関する視点であるのに対し、視点③は緊急時における対策に関する視点である。

第４に、他社の営業秘密の侵害者であると疑われないようにすることや、疑

われた場合に不正を行っていないことを証明できるようにしておく視点も重要である（視点④）。

営業秘密侵害の被疑侵害者となる場面においては、企業の情報管理の高度化が進む中、推定規定の導入や営業秘密侵害品の流通規制、営業秘密侵害罪の非親告罪化等が導入された平成27年（2015年）改正不競法下では、他社の営業秘密の侵害者であると疑われないようにすることや、疑われた場合に不正を行っていないことを証明できるようにしておくことが求められることとなったといえる。第三者から情報を取得しうるルートごとに、いかにして不正な取得を防止するか、また、不正な取得、使用を行っていない事実を証明するためにどのような対策が求められるかが問題となる。

以下では、まず、前記視点①に関し、不競法を所管する経済産業省（以下、「経産省」という）知的財産政策室が作成した営業秘密管理指針の概説を中心に基本的な営業秘密管理のあり方を紹介し（第２）、次に、前記視点②に関し、社内における営業秘密管理の構築（第３）、人事・労務面からみた営業秘密管理（第４）、他社（下請先や共同開発の相手方等）からの自社の営業秘密の漏えい防止策について説明する（第５）。さらに、前記視点③に関し、緊急時における営業秘密漏えいへの対応・対策（第６）について説明し、最後に、前記視点④に関し、他社の営業秘密の侵害防止策について解説する（第７）。

第2 経産省ガイドラインと管理体制

1　全面改訂・営業秘密管理指針の概要

(1)　全面改訂の趣旨――「秘密管理性」の解釈明確化

営業秘密管理指針[1]（以下、便宜上、平成27年（2015年）１月の全面改訂前の営業秘密管理指針を「旧指針」、全面改訂後の指針を「新指針」という）は、平成14年（2002年）７月に政府が発表した知的財産戦略大綱において、「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」を作成する旨が盛り込まれたことを受けて、平成15（2003年）１月に策定された。旧指針は、秘密管理方法に関し、営業秘密と認められう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、それぞれに具体的な管理方法を列挙していたが、新指針では、首相官邸知的財産戦略本部「知的財産推進計画2014」による指摘を受け、事業者にとってわかりやすい内容とするため、前者のみの水準を示すものとした。後者は、別途策定された経産省「秘密情報の保護ハンドブック」[2]によって示されている。

1　経産省が公表している情報管理に関するガイドラインとしては、営業秘密管理指針や秘密情報の保護ハンドブックのほかに、①個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（対象が個人情報に限定）、②組織における内部不正防止ガイドライン（主に従業員等の内部者による不正防止指針。内容がやや概括的である）、③技術流出防止指針（技術流出の防止の観点から好ましい対策例を記載している。特に、組織的、人的アプローチの重要性を強調している）、④情報セキュリティ関連法令の要求事項集（法令上求められる情報セキュリティの水準や法的問題について解説している）などがある。また、企業が構築した情報セキュリティ・マネジメントシステムがJIS Q27001に適合していることを一般財団法人日本情報処理開発協会（JIPDEC）の認証した認証機関が認証する制度であるISMS（Information Security Management System）適合性評価制度（ISMS）は、取扱い情報の機密性、完全性、および可用性等を判断対象としており、多くの部分で秘密管理性の充足性の判断要素と重なる。

2　経産省「秘密情報の保護ハンドブック――企業価値向上に向けて（平成28年２月）」〈www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf〉。

⑵　新指針が規定する秘密管理措置の内容――合理的な努力による認識可能性の確保

新指針は、「秘密管理性要件が満たされるためには、営業秘密保有企業の秘密管理意思が秘密管理措置によって従業員等に対して明確に示され、当該秘密管理意思に対する従業員等の認識可能性が確保される必要がある」としたうえで、秘密管理措置は、対象情報（営業秘密）の一般情報（営業秘密ではない情報）からの合理的区分と当該対象情報について営業秘密であることを明らかにする措置とで構成されるとする（新指針６頁13行以下）。合理的区分とは、企業の秘密管理意思の対象（従業員にとっての認識の対象）を従業員に対して相当程度明確にする観点から、営業秘密が、情報の性質、選択された媒体、機密性の高低、情報量等に応じて、一般情報と合理的に区分されることをいい、営業秘密であることを明らかにする措置としては、主として、媒体の選択や当該媒体への（秘密であることの）表示、当該媒体に接触する者の限定、ないし、営業秘密たる情報の種類・類型のリスト化等が想定されるとする（新指針７頁６行以下）。新指針では、紙媒体の場合、電子媒体の場合、金型や試作品等に情報が化体している場合、および記録化されていない情報の場合について、管理方法が記載されている。たとえば、紙媒体の場合であれば、当該文書に「マル秘」など秘密であることを表示する、施錠可能なキャビネットや金庫等に保管するといった方法があげられている（新指針９頁５行以下）。

⑶　企業秘密を企業内外で共有する場合の秘密管理性の考え方

新指針は、社内の複数箇所で同じ情報を保有しているケースにつき、秘密管理性の有無は、法人全体で判断されるわけではなく、営業秘密たる情報を管理している独立単位（管理単位）ごとに判断されるとし、複数の法人間で同一の情報を保有しているケースにつき、法人（具体的には管理単位）ごとに判断され、別法人における管理状況は原則として影響しないとしている（新指針12頁下から２行以下）。

⑷　新指針の位置づけ――不競法を所管する経産省による法的拘束力のない指針

営業秘密管理指針は、不競法を所管する経産省が、従前の裁判例等を踏まえ、営業秘密の要件（特に「秘密管理性」）について考え方をわかりやすく示しているが、法的拘束力をもつものではなく、個々の紛争事案における判断は、裁判

所により下される。これは新指針でも同様である。

2　新指針に基づく管理体制のチェック

新指針は、秘密管理性の要件をわかりやすくかつ簡潔に解説することを目的としており、細かい法律知識に乏しい多忙な中小企業の経営者でも十分に理解可能な指針を提示しようとしている。情報資産を重要な経営資源とするものの、これまで自社の営業秘密管理に力を注いでこなかった経営者は、今般の全面改訂を機に、同指針の要求する最低水準をクリアしているかどうかチェックすべきといえよう。

手順としては、まず、会社が保有する情報の中で秘匿すべき情報（技術情報、営業情報を含む。なお、旧指針71頁は一般的に営業秘密として管理される情報として〔図表18〕の分類を示している）を抽出し、それがどのような媒体に化体しているかを確認したうえで、媒体ごとに新指針のあげる管理方法のうちいずれかを実践できているかどうかチェックしていくことになる。どの管理方法を選択すべきかは個々の事業者の判断に委ねられているが、当該情報が企業にとってどれだけ重要かという「重要性」の視点、当該管理方法が管理コストや業務効率にどれだけ影響を与えるかという「効率性」の視点、当該管理方法が漏えいリスク回避のためにどれだけ資するかという「実効性」の視点から考えて、最

〔図表18〕　旧指針による営業秘密として管理される情報

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 計画など
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、仕入先情報など
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・経理など）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

も好ましい方法（複数も可）を採用することが望ましいと思われる。また、何を秘匿すべき情報とするかの決定権者をあらかじめ決めておく（必要に応じて「情報セキュリティ委員会」等の組織を設ける）こと、および、秘匿すべき情報とその管理方法が決定したら、それを関係者に周知徹底することも不可欠である。

新指針は、情報に接する従業員の、企業が秘密管理する情報であるということの認識可能性を基準とするとしているが（新指針５頁１行以下）、他方で、企業が秘密管理に向けた合理的な努力をする必要があることも指摘している（同５頁脚注５）。むろん、企業規模や対象となる情報の内容・性質によってその要求される程度は異なりうるが、不競法の条文が「秘密として管理」することを要求しているからには、秘密の保持に向けた積極的な措置が必要である。経営者が当該情報を重要であると考えているだけでは秘密管理性は肯定されないと考えるべきである（同５頁10行以下）。

一方、新指針が指摘するとおり（新指針７頁１行以下）、「職務上知り得た情報全て」「事務所内の資料全て」といった形で秘密表示等を行っているにもかかわらず、情報の内容から当然に一般情報であると従業員が認識する情報が多く含まれるような場合には、「秘密管理措置の形骸化」が生じてしまうこともありうる。何にでも「社外秘」と表示してしまうと、従業者をして秘密とすべき情報とそうでない情報との識別を困難ならしめ、ひいては秘密管理性の成否に悪影響を及ぼすことがありうることに留意すべきである[3]。

また、新指針が指摘するとおり（新指針11頁16行以下）、従業員が体得した無形のノウハウや従業員が職務として記憶した顧客情報等を会社の営業秘密（財産）として確保しておくためには、従業員の退職後の職業選択の自由等との関係から、原則として、その内容自体ないしそのカテゴリーをリスト化したもの（たとえば、「化合物Ｘの製造工程Ｙにおいて成分Ｚを混入する際の諸条件（加熱温度、加熱速度、雰囲気ガスの成分割合等を含む）」といったカテゴリーを箇条書きにしてリスト化することが考えられる）を紙その他の媒体に可視化しておくことが

3　なお、特に大企業では、「極秘」「秘密」「社外秘」といった秘密区分を設けているケースが多いと思われるが、各部署において社内規則に即した秘密指定がなされているか、また、指定がなされている文書について社内規則に従った取扱いがなされているかを調査し、必要に応じて社内規則の見直しや従業員に対し適切な運用の周知徹底を行うことも有用であろう。

〔図表19〕　新指針による媒体別の典型的な管理方法

媒　体	典型的な管理方法	追加的な措置
紙媒体	○ファイルの利用等により一般情報からの合理的な区分を行ったうえで、当該文書に「マル秘」など秘密であることを表示する ○個別の文書やファイルに秘密表示をする代わりに、施錠可能なキャビネットや金庫等に保管する	○紙媒体のコピーやスキャン・撮影の禁止、○コピー部数の管理（余部のシュレッダーによる廃棄）、○配布コピーの回収、○キャビネットの施錠、○自宅持ち帰りの禁止
電子媒体	○電子ファイル名・フォルダ名へのマル秘の付記 ○営業秘密たる電子ファイルを開いた場合に端末画面上にマル秘である旨が表示されるように、当該電子ファイルの電子データ上にマル秘を付記（ドキュメントファイルのヘッダーにマル秘を付記等） ○営業秘密たる電子ファイルそのものまたは当該電子ファイルを含むフォルダの閲覧に要するパスワードの設定 ○記録媒体そのものに表示を付すことができない場合には、記録媒体を保管するケース（CD ケース等）や箱（部品等の収納ダンボール箱）に、マル秘表示を貼付	○人事異動・退職ごとのパスワード変更、○メーラーの設定変更による私用メールへの転送制限、○物理的に USB やスマートフォンを接続できないようにする
物件に営業秘密が化体している場合	○扉に「関係者以外立入禁止」の貼り紙を貼る ○警備員をおいたり、入館 ID カードが必要なゲートを設置したりして、工場内への部外者の立ち入りを制限する ○写真撮影禁止の貼り紙をする ○営業秘密に該当する物件を営業秘密リストとして列挙し、当該リストを営業秘密物件に接触しうる従業員内で閲覧・共有化する	
媒体が利用されない場合	○原則として、下記のような形で、その内容を紙その他の媒体に可視化することが必要となる。（媒体としての管理は上述に従う） －営業秘密のカテゴリーをリストにする －営業秘密を具体的に文書等に記載する ○営業秘密の範囲が従業員にとって明らかな場合は、内容そのものが可視化されていなくとも、当該情報の範囲・カテゴリーを口頭ないし書面で伝達することでも可	

必要となると考えるべきである。

後記する経産省「秘密情報の保護ハンドブック」の「参考資料２」では、「極秘」と「対外秘」の２分類を設け、「極秘」は社内でアクセスできる者を限定して、情報を施錠管理し、複製や社外への持出しを原則的に禁止する情報、「対外秘」は対外的に秘密として保持する情報であり、複製や社外への持出しは必要最低限にすることが求められる情報としたうえで、秘密情報の分類に応じた情報漏えい対策を定める規程として、情報管理基準が例示されている（資料編（資料３））。

3　重要な情報にはより高度な管理方法をとるべきである

新指針は、あくまで秘密管理の最低水準を提示するのみである（新指針１頁下から４行以下）。自社の競争力の源泉となるような重要な情報は、漏えいリスクを最小化するために、新指針が追加的な措置として提示している方法（〔図表19〕右欄参照）や、「秘密情報の保護ハンドブック」が示す管理方法なども参考にしつつ、後記第３で取り上げる対策を適宜実施すべきである。

旧指針は、秘密管理方法として、①秘密指定、アクセス権者の指定、②物理的・技術的管理、③人的管理[4]、④営業秘密侵害に備えた証拠確保等に関する管理[5]、⑤組織的管理[6]をあげていたが、新指針は、このうち③、④および⑤を明示的には要求していない。漏えいリスクを最小化する観点からは、中小企業に比べると人的関係が希薄になりがちな大企業においては特に、他の管理方法に加えて、部門ごとに責任者をおくことや内部監査等を実施するなどの⑤の組

4　誰がどのような営業秘密を扱っているかを把握したうえで、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・研修等を行うこと、また、従業者、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ことを指す。

5　具体的には、営業秘密が記載・記録されている書面、記録媒体等を、閲覧・複製・持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者等のコンピュータの利用状況や通信の記録を保存するといった方法がある。

6　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、①管理方針等（基本方針、規程等）の整備、②責任者の存在とその権限の明確化、③営業秘密侵害を防止するための教育および管理方針等の周知・徹底、④日常的なモニタリングの実施、⑤内部監査の実施、⑥事後対応体制の整備の６項目があげられている。ISMS（前掲（注１）参照）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。

織的管理を補充的に実施することが有意義なことも多い。

また、③の人的管理には、従前の裁判例では、守秘義務を規定する就業規則や退職時の秘密保持誓約書と、物理的な管理がなされていたことの双方を根拠として秘密管理性を肯定しているものも多く、また、人的管理が不十分であった点から秘密管理性を否定する根拠の一つとする裁判例もある[7]。何より、情報漏えいの最たる例は、元従業員や従業員による漏えいである[8]。そして、営業秘密管理に関する社内規則を制定することは有意義であるが、それだけでは、従業員に営業秘密管理に対する意識を植え付けるには不十分である。したがって、情報漏えいを未然に防ぐ見地からは、営業秘密に関する社内規則の策定[9]と従業員への定期的な研修・教育[10]および採用時、退職時等の秘密保持に関する誓約書[11]の提出を中心とする人的管理は、軽視されてはならない。従業員への研修・教育においては、誰がどのような営業秘密を扱っているかを把握したうえで、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

7　たとえば、東京地判平成25・６・26裁判所 HP〔プログラム不正アクセス事件〕は、「本件プログラムには、本件 URL を入力することでアクセスすることが可能な状態であったこと、秘密保持契約を締結するなど、被告に何らの義務を課することもなく、本件 URL は既に同年１月16日には被告に対して開示されていたこと、原告は同年５月31日付け内容証明郵便において被告に対しアクセスを禁止する旨を通知したものの、その後も、本件プログラムへのアクセスに関し、特段の措置を講じていなかったことが認められるから……秘密として管理されていたものということはできない」とする。

8　三菱 UFJ リサーチ＆コンサルティング「人材を通じた技術流出に関する調査研究報告書（別冊）――営業秘密の管理実態に関するアンケート調査結果（平成25年３月）」〈http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/H2503chousa.pdf〉52頁参照。

9　社内規則（就業規則、営業秘密管理規程等）の内容は、前掲（注２）「秘密情報の保護ハンドブック」添付の「各種契約書等の参考例」等が参考になる。また、退職者に退職後競業避止義務を課す場合の留意点や運用の実態については、横地大輔「従業員等の競業避止義務等に関する諸論点について(上)」判タ1387号（2013年）５頁、前掲（注２）「秘密情報の保護ハンドブック」添付の「競業避止義務契約の有効性について」、三菱 UFJ リサーチ＆コンサルティング「人材を通じた技術流出に関する調査研究報告書（平成25年３月）」〈http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/houkokusho130319.pdf〉等が参考になる。

10　中小企業における比較的簡単な教育の例としては、「企業秘密に関する社員心得第○箇条」などのように、企業秘密の管理上重要な事項を箇条書きでまとめ（たとえば、「第１条：余分なコピーを行わない、第２条：移動中は仕事の話はしない」など）、それを月１回の朝礼で読み合わせする、などの対応が考えられる。

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、自社の営業秘密およびその秘密管理の重要性、漏えいした場合のリスク（会社の損害）および法的責任（不競法違反による民事・刑事責任、懲戒処分等）、秘密管理組織の概要、並びに適用される秘密管理ルールを理解させるべく、教育・研修等を行うといったことが考えられる。研修・教育を通じて、従業員に、従業員が業務上取り扱っている情報が会社に帰属する情報であることの意識を植え付けることができ、それが、退職者による情報漏えい防止につながることになる。

4　経産省「秘密情報の保護ハンドブック」

経産省は、営業秘密として法的保護を受けられる水準を超えて、秘密情報の漏えいを未然に防止するための対策を講じようとする企業の参考に資するよう、さまざまな対策例を集めて紹介する「秘密情報の保護ハンドブック」を公表し[12]、各社の事業規模や取り扱う情報の性質などに応じて取捨選択し、情報漏えいの防止に取り組んでいただきたいとしている。同ハンドブックは、場所・状況・環境に潜む「機会」が犯罪を誘発するという犯罪学の考え方なども参考としながら、秘密情報の漏えい要因となる事情を考慮し、①接近の制御、②持出し困難化、③視認性の確保、④秘密情報に対する認識向上（不正行為者の言い逃れの排除）、⑤信頼関係の維持・向上等の５点の「対策の目的」を設定したうえで、それぞれに係る対策を提示している。なお、同ハンドブックについては、そのダイジェスト版も公表されている[13]。

【５つの「対策の目的」】

(1)　接近の制御

秘密情報を閲覧・利用等することができる者（アクセス権者）の範囲を適切に設定した上で、施錠管理・入退室制限等といった区域制限（ゾーニング）等

11　ひな形は、前掲（注２）「秘密情報の保護ハンドブック」別紙「各種契約書等の参考例」９頁以下等が参考になる。

12　かかる見地から、同ハンドブックでは「営業秘密」ではなく、「秘密情報」という言葉が用いられている。

13　経済産業省ホームページ〈www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf〉

により自らが権限を有しない秘密情報に現実にアクセスできないようにすることで、アクセス権限を有しない者を対象情報に近づけないようにすることを目的としています。

なお、「接近の制御」に係る対策のポイントは、まず、アクセス権を有する者が、本当にその情報について知るべき者かという観点から適切に限定されることであり「接近の制御」に係る対策を講ずる前提として、まずは社内の規程等により、アクセス権設定に係るルールを策定することが必要となります。

⑵　持出し困難化

秘密情報が記載された会議資料等の回収、事業者が保有するノート PC の固定、記録媒体の複製制限、従業員の私物 USB メモリ等の携帯メモリの持込み・利用を制限すること等によって、当該秘密情報を無断で複製したり持ち出すことを物理的、技術的に阻止することを目的としています。

⑶　視認性の確保

職場のレイアウトの工夫、資料・ファイルの通し番号管理、録画機能付き防犯カメラの設置、入退室の記録、PC のログ確認等により、秘密情報に正当に又は不当に接触する者の行動が記録されたり、他人に目撃されたり、事後的に検知されたりしやすい環境を整えることによって、秘密情報の漏えいを行ったとしても見つかってしまう可能性が高い状態であると認識するような状況を作り出すことを目的としています。また、ここでの対策は、従業員等の行為の正当性（身の潔白）を証明する手段としても有効です。

さらに、現実に監視するというだけでなく、例えば、職場の整理整頓や従業員等に文書管理責任を分担させて情報管理に関する当事者意識を持たせたりすることで、職場を管理の行き届いた状態にすることにより心理的に漏えいしにくい状況を作ることも含まれます。

なお、情報漏えい行為の状況などを記録する対策等は、情報漏えいが生じた場合の行為者に対する責任追及の際に必要となる証拠の確保手段としての意義もあります。

⑷　秘密情報に対する認識向上（不正行為者の言い逃れの排除）

秘密情報の取扱い方法等に関するルールの周知、秘密情報の記録された媒体へ秘密情報である旨の表示を行うこと等により、従業員等の秘密情報に対する認識を向上させることを目的としています。これにより、同時に、不正に情報漏えいを行う者が「秘密情報であることを知らなかった」、「社外に持ち出してはいけない資料だと知らなかった」、「自身が秘密を保持する義務を負っている

情報だとは思わなかった」といった言い逃れができないようになります。

⑸　信頼関係の維持・向上等

従業員等に情報漏えいとその結果に関する事例を周知することで、秘密情報の管理に関する意識を向上させます。また、働きやすい職場環境の整備や適正な評価等によって企業への帰属意識を醸成したり、仕事へのモチベーションを向上させます。これらの取組みによって、職場のモラルや従業員等との信頼関係を維持・向上することを目的とします。

従業員等との信頼関係を維持・向上するための取組みは、企業の生産性向上や効率的な経営の実現などの観点からも重要なポイントであるため、企業においては既に創意工夫を凝らしながら様々な取組みが実施されているところですが、これらの取組みが、情報漏えい対策としても有効であると考えられます。

出典：経産省「秘密情報の保護ハンドブック」18～20頁

【執筆者略歴】（執筆順）

服 部　　誠（はっとり　まこと）

弁護士・弁理士・ニューヨーク州弁護士（阿部・井窪・片山法律事務所・パートナー）
神戸大学大学院法学研究科客員教授、慶應義塾大学理工学部修士課程講師、一橋大学大学院国際企業戦略研究科講師

1998年に弁護士登録後、主に企業法務に携わり、情報管理、知的財産、会社法務といった分野に関する訴訟、意見書作成、依頼者からの相談等を多く担当している。経済産業省経済産業政策局知的財産政策室出向時（2001年～2002年）には、営業秘密を規定する不正競争防止法の改正作業に携わった経験を有する。

企業情報管理に関する主要著書／論文に、『逐条解説不正競争防止法〔平成13年改正版〕』（共著・有斐閣、2002年）、『企業情報管理実務マニュアル――漏えい・事故リスク対応の実務と書式』（分担執筆・民事法研究会、2015年）、「弁護士からみた実務上の留意点（特集 全面改訂・営業秘密管理指針の対応）」NBL 1045号（2015年）、「平成27年改正不正競争防止法における営業秘密の保護」自由と正義 2012年 1 月号（日本弁護士連合会）等がある。

第１章第１～第３、第２章、第３章第１・第２・第４・第６・第７担当

小 林　　誠（こばやし　まこと）

デロイト トーマツ ファイナンシャルアドバイザリー合同会社
シニアヴァイスプレジデント
K.I.T. 虎ノ門大学院（金沢工業大学大学院）イノベーションマネジメント研究科客員教授、東京工業大学環境・社会理工学院技術経営専門職課程 CUMOT プログラム知的財産戦略コース講師、知的財産アナリスト認定講座（AIPE 認定シニア知的財産アナリスト）講師、トレードシークレット・マネージャー養成講座講師

国際特許事務所を経て2007年に現職に至り、知的財産が重要となる製造業およびICT 業界のクロスボーダーM&A におけるファイナンシャルアドバイザリー、および知的財産戦略コンサルティング業務を専門としている。

近年はプロスポーツ業界における新会社設立やブランド・コンテンツの価値評価、ゲームソフトメーカーの知的財産管理体制構築支援、放送事業者のコンテンツ二次利用の拡大を目的とした分社化支援、大手製造業における営業秘密管理体制構築支援などにも従事している。

主な著書に『知財戦略のススメ――コモディティ化する時代に競争優位を築く』（共著・日経BP社、2016年）等がある。

第１章第１、第３章第３担当

岡 田 大 輔（おかだ　だいすけ）

デロイト トーマツ ファイナンシャルアドバイザリー合同会社
シニアヴァイスプレジデント
公認不正検査士
トレードシークレット・マネージャー養成講座講師

消費者金融業、輸入卸業、人材派遣業等を経て、2008年よりデジタル・フォレンジック業界に身を投じ、2013年より現職に至る。産業スパイ、情報漏えい等の事案に対するデジタル・フォレンジックを活用した不正調査を得意としており、これまでに指揮を執った事案は述べ200件を超え、それらの調査から発展した訴訟支援も多数経験している。その経験を活かし、営業秘密の専門家として、企業における営業秘密漏えいのインシデント対応、漏えい対策、管理体制構築などの分野で活動している。

第３章第３・第５担当

泉　　修 二（いずみ　しゅうじ）

デロイト トーマツ ファイナンシャルアドバイザリー合同会社
シニアヴァイスプレジデント
公認不正検査士

大手通信キャリアにおいて、全国通信バックボーンの設計・運用、他事業者との相互接続ネットワークにおける技術仕様検討、無線技術検討などのネットワークエンジニアリングを経験後、広報の技術領域担当者としてマスメディア対応に従事。

現在は、デジタル・フォレンジックによる不正調査対応、e-Discovery 対応の傍ら、リスクアセスメントおよびインシデント発生を見据えた対外的情報発信における体制構築や情報統制などの支援も担当し、数々のインシデント事案においてサービス提供の実績を有する。

第３章第５担当

営業秘密管理実務マニュアル

平成29年２月13日　第１刷発行

定価　本体2,800円 +税

著　者　　服部誠・小林誠・岡田大輔・泉修二
発　行　　株式会社　民事法研究会
印　刷　　藤原印刷株式会社

発行所　　株式会社　民事法研究会
〒150-0013　東京都渋谷区恵比寿3-7-16
〔営業〕TEL 03(5798)7257　FAX 03(5798)7258
〔編集〕TEL 03(5798)7277　FAX 03(5798)7278
http://www.minjiho.com/　info@minjiho.com

落丁・乱丁はおとりかえします。　ISBN978-4-86556-138-8　C2032　¥2800E
カバーデザイン：関野美香