営業秘密管理指針

平成１５年１月３０日

（最終改訂：平成３１年１月２３日）

経済産業省

（改訂履歴）

平成１７年１０月１２日改訂
平成２２年　４月　９日改訂
平成２３年１２月　１日改訂
平成２５年　８月１６日改訂
平成２７年　１月２８日改訂
平成３１年　１月２３日改訂

目　次

はじめに（本指針の性格）

○（本指針の位置づけ）

・ 本指針は、経済産業省が、不正競争防止法を所管し、また、TRIPS 協定など通商協定を所掌する行政の立場から、企業実務において課題となってきた営業秘密の定義等（不正競争防止法による保護を受けるための要件など）について、イノベーションの推進、海外の動向や国内外の裁判例（日本における最高裁判所の判例は改訂時点で存在しない）等を踏まえて、一つの考え方を示すものであり、法的拘束力を持つものではない。

・ したがって、当然のことながら、不正競争防止法に関する個別事案の解決は、最終的には、裁判所において、個別の具体的状況に応じ、他の考慮事項とともに総合的に判断されるものである。

○（改訂の経緯）

・ 本指針は、「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」として平成１５年１月に策定された「営業秘密管理指針」[1]を平成２７年に全面的に改訂したものである。

・ 平成２７年の全面改訂に当たっては、「知的財産推進計画 2014」（平成２６年７月知的財産戦略本部決定）で、「一部の裁判例等において秘密管理性の認定が厳しいとの指摘や認定の予見可能性を高めるべきとの指摘があることも視野に入れつつ、営業秘密管理指針において、法的に営業秘密として認められるための管理方法について、事業者にとってより分かりやすい記載とするよう改める」と記載されたことを踏まえ、産業構造審議会知的財産分科会営業秘密の保護・活用に関する小委員会（以下、「営業秘密小委」という。）において議論いただいた。

・ その後、ビッグデータ、AI の活用が推進する第四次産業革命を背景として情報活用形態が多様化する状況を踏まえて、営業秘密小委において議論が行われ、営業秘密の管理の実態に即した「営業秘密管理指針」の見直しの方向性が示された（平成２９年５月公表「第四次産業革命を視野に入れた不正競争防止法に関する検討　中間とりまとめ[2]」）。これを受け、平成３０年１月に本指針が改訂された。

○（指針で示す管理水準）

---

[1] 平成２７年１月まで、裁判例の蓄積や不正競争防止法の改正等に対応した改訂を４回実施。

[2] http://www.meti.go.jp/report/whitepaper/data/20170509001.html

・　本指針は、不正競争防止法によって差止め等の法的保護を受けるために必要となる最低限の水準の対策を示すものである。漏えい防止ないし漏えい時に推奨される（高度なものを含めた）包括的対策については、「秘密情報の保護ハンドブック（平成２８年２月）」に掲載されている[3]。

[3] 「秘密情報の保護ハンドブック」は以下に掲載。
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf
さらに同ハンドブックの簡易版として策定した「秘密情報の保護ハンドブックのてびき」は以下に掲載。
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/170607_hbtebiki.pdf

１．総説

○（不正競争防止法の位置付け）

・　不正競争防止法は、他人の技術開発、商品開発等の成果を冒用する行為等を不正競争として禁止している。具体的には、ブランド表示の盗用、形態模倣等とともに、営業秘密の不正取得・使用・開示行為等を差止め等の対象としており、不法行為法の特則として位置づけられるものである。

○（不正競争防止法における営業秘密の定義）

・　不正競争防止法（以下、「法」という。）第２条第６項は、営業秘密を
①秘密として管理されている［秘密管理性］
②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、
③公然と知られていないもの［非公知性］
と定義しており、この三要件全てを満たすことが法に基づく保護を受けるために必要となる。

・　また、本三要件を含めた法における営業秘密の保護規定は、加盟国間の最低限の保護水準を定めた「知的所有権の貿易関連の側面に関する協定」（ＴＲＩＰＳ協定。1987 年から行われた交渉を踏まえ、我が国は 1995 年に加入）を担保する性格を持つものであり、法の解釈に当たっては、最低限の保護水準を示す同協定の存在に留意する必要がある。なお、本三要件と実質的に同趣旨の要件が、諸外国においても営業秘密保護の条件とされている（ただし、運用には幅がある）。

（参考）ＴＲＩＰＳ協定条文（抄）

第七節 開示されていない情報の保護

第三十九条

1967 年のパリ条約第十条の二に規定する不正競争からの有効な保護を確保するために、加盟国は、開示されていない情報を 2 の規定に従って保護し、及び政府又は政府機関に提出されるデータを 3 の規定に従って保護する。

２．自然人又は法人は、合法的に自己の管理する情報が次の(a)から(c)までの規定に該当する場合には、公正な商慣習に反する方法により自己の承諾を得ないで他の者が当該情報を開示し、取得し又は使用することを防止することができるものとする。

（ａ）当該情報が一体として又はその構成要素の正確な配列及び組立てとして、当該情報に類する情報を通常扱う集団に属する者に一般的に知られておらず又は容易に知ることができないという意味において秘密であること。

（b）秘密であることにより商業的価値があること。
（c）当該情報を合法的に管理する者により、当該情報を秘密として保持するための、状況に応じた合理的な措置がとられていること。

○営業秘密と民事・刑事上の措置との関係

・ 営業秘密に該当すれば、法に基づく差止めをはじめとする民事上、刑事上の措置の対象になりうることとなる。

・ もっとも、秘密管理性等の三要件が認められ、営業秘密に該当したとしても差止め等や刑事措置の対象となるためには、法に定められる「不正競争」や「営業秘密侵害罪」としての要件をすべて充足しなければならない（法第２条第１項第４号～第１０号、法第２１条第１項各号等）ことに留意する必要がある。

○契約による情報の保護

・ 営業秘密に該当しない情報については、法による保護を受けることはできないものの、民法その他による法的保護を一切受けることができないわけではない。すなわち、当該情報の取扱いについて私人間の契約において別途の規律を設けた場合には、当該契約に基づく差止め等の措置を請求することが可能であり、その際、法における営業秘密に該当するか否かは基本的には関係がないと考えられることに留意する必要がある。

２．秘密管理性について

（１）秘密管理性要件の趣旨

秘密管理性要件の趣旨は、企業が秘密として管理しようとする対象（情報の範囲）が従業員等に対して明確化されることによって、従業員等の予見可能性、ひいては、経済活動の安定性を確保することにある。

○（営業秘密の情報としての特性）

・ 営業秘密は、そもそも情報自体が無形で、その保有・管理形態も様々であること、また、特許権等のように公示を前提とできないことから、営業秘密たる情報の取得、使用又は開示を行おうとする従業員や取引相手先（以下、「従業員等」という。）にとって、当該情報が法により保護される営業秘密であることを容易に知り得ない状況が想定される。

○（秘密管理性要件の趣旨）

・　秘密管理性要件の趣旨は、このような営業秘密の性質を踏まえ、企業が秘密として管理しようとする対象が明確化されることによって、当該営業秘密に接した者が事後に不測の嫌疑を受けることを防止し、従業員等の予見可能性、ひいては経済活動の安定性を確保することにある[4]。

○（留意事項）

・　秘密管理性要件については、企業が、ある情報について、相当高度な秘密管理を網羅的に行った場合にはじめて法的保護が与えられるべきものであると考えることは、次の理由により、適切ではない[5]。

- 現実の経済活動において、営業秘密は、多くの場合、それを保有する企業の内外で組織的に共有され活用されることによってその効用を発揮する。企業によっては国内外の各地で子会社、関連会社、委託先、又は、産学連携によって大学などの研究機関等と営業秘密を共有する必要があるため、リスクの高低、対策費用の大小も踏まえた効果的かつ効率的な秘密管理の必要があること。

- 営業秘密が競争力の源泉となる企業、特に中小企業が増加しているが、これらの企業に対して、「鉄壁の」秘密管理を求めることは現実的ではない。仮にそれを求めることになれば、結局のところ、法による保護対象から外れてしまうことが想定され、イノベーションを阻害しかねないこと。

- 下請企業についての情報や個人情報などの営業秘密が漏えいした場合、その被害者は営業秘密保有企業だけであるとは限らないこと。

4　秘密管理性要件の趣旨として、適切に管理がなされていない情報は、早晩他社に知られてしまい、競争優位性が失われることとなるとの前提に立ち、そのような情報に法的保護を与えたとしても研究・開発のインセンティブが図られないことから、企業が特定の情報を秘密として管理しようとする合理的な自助努力に対して法的保護を与えようとしたものとの考え方も成り立ちうる（例えば、田村善之「営業秘密の秘密管理性要件に関する裁判例の変遷とその当否－主観的認識 vs.「客観的」管理－」知財管理 64 巻 5 号～6 号）。この点、本指針は、あくまで従業員の予見可能性の確保を中心に説明することから、同見解とは若干異なる面がある。

5 別の政策論としては、秘密管理措置の有無にかかわらず、従業員が、企業にとって秘密である（秘密としたい）ことを知って取得した情報については、当該従業員にとっては営業秘密性を認め、民事・刑事上の措置の対象とするべきとする考え方もある。しかし、現行法の「秘密として管理されている」という文言と必ずしもそぐわない上、このような考え方を採用した場合、従業員の主観という事後的に検証が困難な事実に依存することになるため、予見可能性が乏しく、経済活動の安定性や円滑な転職を害するおそれがあるものと考えられる。

（２）必要な秘密管理措置の程度

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。

具体的に必要な秘密管理措置の内容・程度は、企業の規模、業態、従業員の職務、情報の性質その他の事情の如何によって異なるものであり、企業における営業秘密の管理単位（本指針１４頁参照）における従業員がそれを一般的に、かつ容易に認識できる程度のものである必要がある。

○（総説）

・　秘密管理性要件が満たされるためには、営業秘密保有企業が当該情報を秘密であると単に主観的に認識しているだけでは不十分である。

すなわち、営業秘密保有企業の秘密管理意思（特定の情報を秘密として管理しようとする意思）が、具体的状況に応じた経済合理的な秘密管理措置[6]によって、従業員に明確に示され、結果として、従業員が当該秘密管理意思を容易に認識できる（換言すれば、認識可能性が確保される）必要がある。

取引相手先に対する秘密管理意思の明示についても、基本的には、対従業員と同様に考えることができる。

○（秘密管理措置の対象者）

・　秘密管理措置の対象者は、当該情報に合法的に、かつ、現実に接すること

---

6 秘密管理性要件は、従来、①情報にアクセスできる者が制限されていること（アクセス制限）、②情報にアクセスした者に当該情報が営業秘密であることが認識できるようにされていること（認識可能性）の２つが判断の要素になると説明されてきた。しかしながら、両者は秘密管理性の有無を判断する重要なファクターであるが、それぞれ別個独立した要件ではなく、「アクセス制限」は、「認識可能性」を担保する一つの手段であると考えられる。したがって、情報にアクセスした者が秘密であると認識できる（「認識可能性」を満たす）場合に、十分なアクセス制限がないことを根拠に秘密管理性が否定されることはない。

もっとも、従業員等がある情報について秘密情報であると現実に認識していれば、営業秘密保有企業による秘密管理措置が全く必要ではないということではない。法の条文上「秘密として管理されている」と規定されていることを踏まえれば（法第２条第６項）、何らの秘密管理措置がなされていない場合には秘密管理性要件は満たさないと考えられる。

なお、「アクセス制限」の用語は権限のない者が情報にアクセスすることができないような措置を講じることという語義で使用されることが多いが、秘密として管理する措置には、「秘密としての表示」や「秘密保持契約等の契約上の措置」も含めて広く考えることが適当である。それを明確化するため、本指針においては「アクセス制限」ではなく、「秘密管理措置」という用語で説明する。

ができる従業員等である。
　職務上、営業秘密たる情報に接することができる者が基本となるが、職務の範囲内か否かが明確ではなくとも当該情報に合法的に接することができる者（例えば、部署間で情報の配達を行う従業員、いわゆる大部屋勤務において無施錠の書庫を閲覧できる場合における他部署の従業員など）も含まれる。

・　従業員に対する秘密管理措置があれば、侵入者等（住居侵入罪にあたる行為により情報に接触する者など法第２条第１項第４号及び第２１条第１項第１号にいう詐欺等行為又は管理侵害行為等によって営業秘密を取得しようとする者）に対しても秘密管理性は確保されるのであって、営業秘密保有企業の秘密管理意思が従業員に対するものとは別に侵入者等に示される（別の秘密管理措置が行われる）必要はない。
※注　侵入者に対する刑事罰については、故意及び図利加害目的の要件を追加的に満たす必要がある。

○（合理的区分）
・　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。

・　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う。
※注　営業秘密保有企業が営業秘密たる情報のみを保有し、営業秘密たる情報以外の情報を保有しないことは考えにくいため、秘密管理措置の一環として、合理的区分が必要となることが通常である。

・　この合理的区分とは、情報が化体した媒体について、例えば、紙の１枚１枚、電子ファイルの１ファイル毎に営業秘密であるか一般情報であるかの表示等を求めるものではなく、企業における、その規模、業態等に即した媒体の通常の管理方法に即して、営業秘密である情報を含む（一般情報と混在することもありうる。）のか、一般情報のみで構成されるものであるか否かを従業員が判別できればよい（※）。
※注　紙であればファイル、電子媒体であれば社内ＬＡＮ上のフォルダなどアクセス権の同一性に着目した管理がなされることが典型的であるが、業態によっては、書庫に社外秘文書（アクセス権は文書によって異なる）が一括して保存されるケースも存在し、そのような管理も

合理的区分として許容される[7]。ただし、「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著しく多く含まれる場合には、下記留意事項に記載した「秘密管理措置の形骸化」と評価されることもありうる。

○（その他の秘密管理措置）

・ 合理的区分に加えて必要となる秘密管理措置としては、主として、媒体の選択や当該媒体への表示、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、秘密保持契約（あるいは誓約書）などにおいて守秘義務を明らかにする等が想定される。要するに、秘密管理措置の対象者たる従業員において当該情報が秘密であって、一般情報とは取扱いが異なるべきという規範意識が生じる程度の取組であることがポイントとなる。

・ 秘密管理措置の具体的な内容・程度は、当該営業秘密に接する従業員の多寡、業態、従業員の職務、情報の性質、執務室の状況その他の事情によって当然に異なるものであり、例えば、営業秘密に合法的かつ現実的に接しうる従業員が少数である場合において、状況によっては当該従業員間で口頭により「秘密情報であること」の確認をしている等の措置で足りる場合もあり得る。

○留意事項

・ 情報に対する秘密管理措置がその実効性を失い「形骸化」したともいいうる状況で、従業員が企業の秘密管理意思を認識できない場合は、適切な秘密管理措置とはいえない。

※注　一時的ないし偶発的な管理不徹底に過ぎず、当該企業の秘密管理意思に対する従業員の認識可能性に重大な影響を与えない場合まで「形骸化」と評価することは適切ではない。

・ 個人情報保護法で保護される個人情報については、同法で漏えい対策を含む安全管理義務が保有企業に対して義務づけられており、それが従業員にとっても明らかであり、かつ、一般情報との区別も外見上明確であることから、その他の情報に比べて、秘密管理性が認められる可能性が高いものと考えられる。

・ なお、秘密管理性とは別に、企業が社会的責任として講じることが期待さ

[7] このほか、特許出願を行う部署などの一部署を入室制限付きの執務室とし、当該執務室の情報は全てが営業秘密であるとの取扱いが考えられる。

れる情報漏えい防止対策には、その内容は企業の自主的な判断によるものの、漏えいリスクの大小等に応じて、従業員の行動に対する各種の意識啓発[8]、牽制や漏えいの検知等を行って漏えいリスクを減少する方策、又は、被害拡大を防止するための方策が含まれることが通例であり、秘密管理措置とは必ずしも一致しないため留意が必要である。

〈参考裁判例〉

・企業の規模を考慮した例

パスワード等によるアクセス制限、秘密であることの表示等がなかったにもかかわらず、全従業員数が 10 名であり、性質上情報への日常的なアクセスを制限できないことも考慮し、秘密管理性を肯定（大阪地判平成 15 年 2 月 27 日　平成 13 年（ワ）10308 号)。

・営業上の必要性を理由に緩やかな管理を許容した例

顧客情報の写しが上司等に配布されたり、自宅に持ち帰られたり、手帳等で管理されて成約後も破棄されなかったりしていたとしても、これらは営業上の必要性に基づくものであり、従業員が本件顧客情報を秘密であると容易に認識し得るようにしていたとして、秘密管理性を肯定（知財高判平成 24 年 7 月 4 日　平成 23 年（ネ）10084 号)。

・情報の性質から従業員等が認識可能であると認定した例

ＰＣ樹脂の製造技術に関する情報は世界的に希有な情報であって、製造に関係する従業員は当該製造技術が秘密であると認識していたといえるとして秘密管理性を肯定（知財高裁平成 23 年 9 月 27 日　平成 22 年（ネ）10039 号)。

・物理的な管理体制を問題にすることなく秘密管理性を肯定した例

安価で販売して継続的取引を得るなどの極めて効果的な営業活動を可能ならしめるものという情報の重要性と、情報を開示されていたのが従業員１１名に過ぎなかったことに加えて、被告が退職する直前に秘密保持の誓約書を提出させていたこと等の事情を斟酌して、秘密管理性を肯定（大阪高判平成 20 年 7 月 18 日　平成 20 年（ネ）245 号)。

（３）秘密管理措置の具体例

秘密管理措置は、前述（２）のとおり、具体的状況に応じて多様である

[8] 従業員への意識啓発の方法として、労使の対話の場、情報管理ルール等に係る研修、e-ラーニング等の教育プログラムなど様々な機会を捉まえて、営業秘密とは何か、自社の扱う営業秘密の重要性、許される共有の範囲、営業秘密として秘密にしなければならない期間等について、従業員に対する周知を図ることが望ましい。

が、ここでは、一例として媒体に対する典型的な秘密管理措置を紹介する。
※注　秘密管理方法としては、媒体に対するもの以外に、媒体を利用せず無形の情報として管理したり、情報に合法的かつ現実的に接触する者を限定する方法などが想定されることは前述。

①　紙媒体の場合

○典型的な管理方法

・　前述のとおり、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、基本的には、当該文書に「マル秘」など秘密であることを表示することにより、秘密管理意思に対する従業員の認識可能性は確保されると考えられる。

・　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方法も、認識可能性を確保する手段として考えられる。

・　なお、情報の漏えい事案が社内で多発しているなど不正取得のリスクが顕在化している場合に、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といった追加的な措置によって、秘密管理意思の明示がより確固としたものになることは想定される。しかしながら、通常の状況においては、これらの措置は、情報漏えい対策上有効であるとしても、秘密管理性を充足するための必須のものではない。（前述（２）のとおり、秘密管理性とは別に、企業の自主的な漏えいリスク低減のための情報漏えい対策という観点からは更に高度な対策を取るという判断がありうる）

〈参考裁判例〉

・ 人材派遣業を営む会社の従業員が派遣労働者の雇用契約に関する情報等を持ち出した事例において、当該情報は、施錠棚への保管やコピーの制限・回収、秘密表示がなされていなかったが、従業員との秘密保持契約、当該情報の管理に係る一般的な注意喚起等の事情を斟酌し、秘密管理性を肯定（東京地判平成 14 年 12 月 26 日　平成 12 年（ワ）22457 号）。

②　電子媒体の場合

○典型的な管理方法

・　データなどの電子媒体で保管している場合も基本的には紙媒体と同様であ

るが、電子情報の場合は、通常、次のような方法のいずれかによって、秘密管理性の観点から充分な秘密管理措置となり得るものと考えられる。

－記録媒体へのマル秘表示の貼付

－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又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、マル秘表示の貼付

・　また、外部のクラウドを利用して営業秘密を保管・管理する場合も、秘密として管理されていれば、秘密管理性が失われるわけではない。例えば、階層制限に基づくアクセス制御などの措置が考えられる。

・　なお、不正利用・不正取得のリスクが顕在化している場合には、追加的に、人事異動・退職毎のパスワード変更、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こと等によって、秘密管理意思の明示がより確固としたものになることが想定される。しかし、通常の状況においては、これらの措置は、情報漏えい対策上有効であるとしても、秘密管理性を充足するための必須のものではない。（前述（２）のとおり、秘密管理性とは別に、漏えいリスク低減のための情報漏えい対策という観点からは更に高度な対策を取るという判断がありうる）

〈参考裁判例〉

・情報の入ったパソコンのＩＤとパスワードを複数の従業員で共有しており、さらにＩＤとパスワードを付箋に書いて貼ってあり、退職者が出てもＩＤとパスワードが変更されることはなかったという事案において、ＩＤやパスワードの趣旨が有名無実化していたというような事情があればともかく、そのような事情が認められない限り、なお秘密管理性を認めるに妨げないとして秘密管理性を肯定（大阪地判平成 20 年 6 月 12 日　平成 18 年（ワ）5172 号）。

・パスワードが変更されたことはなく、パソコンにパスワードを記載した付せんを貼っている者がおり、プライスリストを印刷したものに「社外秘」等の押印をする取決めはなかった事案において、プライスリストに機械製造業者にとって一般的に重要であることが明らかな仕入原価等の情報が記載されていること等を参酌し、プライスリストの外部への提示や持ち出しが許されていたという事情は認められないとして秘密管理性を肯定（名古屋地判平成 20 年 3 月 13 日　平成 17 年（ワ）3846 号)。

③　物件に営業秘密が化体している場合

・　製造機械や金型、高機能微生物、新製品の試作品など、物件に営業秘密情報が化体しており、物理的にマル秘表示の貼付や金庫等への保管に適さないものについては、例えば、次のような方法のいずれかを講じることによって、秘密管理性の観点から秘密管理措置となりうるものと考えられる。

－扉に「関係者以外立入禁止」の張り紙を貼る

－警備員を置いたり、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

④　媒体が利用されない場合

・　例えば、技能・設計に関するものなど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については、従業員の予見可能性を確保し、職業選択の自由にも配慮する観点（※１）から、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①から③に前述)

－営業秘密のカテゴリーをリストにすること（※２）

－営業秘密を具体的に文書等に記載すること

※注１　これらの情報は、多くの場合、一般情報との区別が困難であるため、当該体得情報を可視化することなくその情報の使用を禁じてし

まうと、従業員にとってはいかなる情報の開示・持ち出しが禁じられているのかが明確でなく、転職自体が困難となりかねない。

※注２　最先端の技術開発現場が典型的であるが、日々高度の営業秘密が創出・更新され、内容の整理分類が常時なされていない状況においては、カテゴリーのリスト化や秘密保持契約（あるいは誓約書）等による範囲の特定が有効であると考えられる。

・　一方で、例えば、未出願の発明や特定の反応温度、反応時間、微量成分、複数の物質の混合比率が営業秘密になっている場合（化学産業などで多く見られる）などで、その情報量、情報の性質、当該営業秘密を知りうる従業員の多寡等を勘案して、その営業秘密の範囲が従業員にとって明らかな場合には、必ずしも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によって、従業員の認識可能性を確保することができるものと考えられる。

・　なお、従業員が体得した情報が営業秘密に該当する場合には、転職後の使用・開示によって、直ちに、民事上及び刑事上の措置の対象となるわけではない。従業員が営業秘密保有企業との関係で信義則上の義務に著しく反するような形で当該営業秘密の取得・使用・開示をした場合に限り、民事上又は刑事上の措置の対象となるのであり、その判断に当たっては、当該企業と従業員との間の信頼関係の程度、当該企業の利益、従業員の利益、営業秘密の内容等を踏まえた総合的な考慮によるものであることに留意が必要である[9]。

⑤　複数の媒体で同一の営業秘密を管理する場合

・　同一の情報を紙及び電子媒体で管理することが企業実務で多く見られるが、複数の媒体で同一の営業秘密を管理する場合には、それぞれについて秘密管理措置が講じられることが原則である。

・　ただし、従業員が同一の情報につき複数の媒体に接する可能性がある場合において、いずれかの媒体への秘密管理措置（マル秘表示等）によって当該情報についての秘密管理意思の認識可能性が認められる場合には、仮にそれ以外の媒体のみでは秘密管理意思を認識しがたいと考えられる場合であっても、秘密管理性は維持されることが通常であると考えられる。

9　従業員の転職に際して、退職従業員による新雇用主への営業秘密開示行為等が、旧雇用主との関係で信義則上の義務に著しく反するような形でなされた場合、新雇用主は、そのような信義則上の義務に著しく反する開示であることについて悪意又は重過失で当該営業秘密を使用等すると営業秘密侵害となる。

（４）営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

企業内（支店、営業所等）、企業外（子会社、関連会社、取引先、業務委託先、フランチャイジー等）と営業秘密を共有する場合においては、次のように整理される。

①　社内の複数箇所で同じ情報を保有しているケース

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（以下、「管理単位」という。）ごとに判断される。当該管理単位内の従業員にとって、当該管理単位における秘密管理措置に対する認識可能性があればよい。

・　支店など社内の複数箇所で同一の営業秘密を保有していた場合、それぞれの箇所で状況に応じた秘密管理措置が講じられる必要がある。しかしながら、いずれかの箇所で秘密管理措置がなされていなければ、（当該箇所では秘密管理性が否定されることは当然であるが）、その他の箇所でも当該情報の秘密管理性が否定されるわけではない。

・　すなわち、管理単位（規模、物理的環境、業務内容も勘案しつつ、秘密管理措置の要否や内容の決定及びその遵守状況の監督（違反者の処分等）に関する自律的決定権限の有無その他の事情の有無から判断して、営業秘密の管理について一定の独立性を有すると考えられる単位。典型的には、「支店」「事業本部」など。）ごとに、当該企業の秘密管理意思に対する認識可能性があればよい。

※注　充分な秘密管理措置が行われているA単位から情報が漏えいした場合において、B単位における秘密管理措置の不存在をもって、A単位の秘密管理性は通常、否定されない。ただし、B単位における秘密管理措置の不存在の事実が、継続的で、社内で公然の事実であるといった状況の結果、A単位の従業員の認識可能性が損なわれている場合には、その後、A単位から情報が漏えいした場合に、A単位における秘密管理性は否定されうる（ただし、各単位における一時的・偶発的な管理不徹底によって秘密管理性が直ちに失われるわけではない）。

②　複数の法人間で同一の情報を保有しているケース

秘密管理性の有無は、法人（具体的には管理単位）ごとに判断され、別法人

内部での情報の具体的な管理状況は、自社における秘密管理性には影響しないことが原則である。

・　**（法人単位での判断）**

子会社をはじめとして、企業外の別法人については、会社法等の法令上、営業秘密保有企業自体が当該別法人の内部における秘密管理措置の実施を直接に実施・確保することはできないこと、法も「保有者」の概念を用いており、事業者単位での管理を想定していると考えられることを踏まえ、別法人内部での情報の具体的な管理状況は、自社における秘密管理性には影響しないことが原則である。

・　**（別法人の不正な使用に対する差止請求等）**

自社の営業秘密について、子会社等の別法人が不正な利用を行っている場合に、自社が当該別法人に対して差止請求等を行うためには、当該別法人（具体的には自社から当該営業秘密を共有した担当者）に対して、自社従業員に対するのと同様に、自社の秘密管理意思が明確に示されている必要がある（法第２条第１項第７号等の「営業秘密を保有者から示された」ことが必要）。

※注　Ｃ社からＤ社に対して営業秘密が示されたケース（Ｄでは当該営業秘密をＤ自身の営業秘密として管理）において、Ｄが営業秘密を漏えいしたＤの従業員に差止め等を求めることの可否は、Ｄ内部の従業員に対する認識可能性の有無の問題となる。

・　具体的には、営業秘密を特定した秘密保持契約（NDA）の締結により自社の秘密管理意思を明らかにする場合が典型的であるが、取引先との力関係上それが困難な場合には、自社では営業秘密として管理されているという事実の口頭による伝達や開示する文書へのマル秘表示によっても、自社の秘密管理意思を示すことは、理論上は可能である。ただし、立証を考慮すれば、口頭での秘密管理意思の伝達ではなく、何らかの書面（送り状への記載等）が望ましい。

※注　営業秘密に該当する場合であっても、その使用等が直ちに民事・刑事上の措置の対象となるわけではない。当事者間の信頼関係の程度、各当事者の利益、営業秘密の内容等を踏まえ信義則に著しく反するなど「不正の利益を得る目的」又は「保有者に損害を加える目的」であると評価される場合にのみ、民事・刑事上の措置の対象となることとなる。

・　また、複数企業で共同研究開発を実施する場合等、複数の他の企業に自社

の営業秘密たる情報を開示することが想定されるが、その場合、自社の秘密管理意思を示すためには、開示先である共同研究開発に参加する複数企業等を当事者としたNDAを締結することが有効であると考えられる。

・　逆に、例えば、別法人と営業秘密を特定したNDAを締結せずに営業秘密を共有した場合など、別法人に対して自社が秘密管理措置を講じていないことを以て、自社における従業員との関係での秘密管理性には影響しないことが原則である。

※注　ただし、仮に、営業秘密保有企業Eが別法人Fに対して、特段の事情が無いにも関わらず、何らの秘密管理意思の明示なく、営業秘密を取得・共有させているような状況において、E企業の一部の従業員が、「特段事情が無いにも関わらず、何らの秘密管理意思の明示なく自社Eの営業秘密をFに取得・共有させた」という状況を認識している場合においては、E企業の従業員の認識可能性が揺らぎ、結果として、Eにおける秘密管理性が否定されることがありうることに注意が必要である。

３．有用性の考え方

「有用性」が認められるためには、その情報が客観的にみて、事業活動にとって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。

（１）「有用性」の要件は、公序良俗に反する内容の情報（脱税や有害物質の垂れ流し等の反社会的な情報）など、秘密として法律上保護されることに正当な利益が乏しい情報を営業秘密の範囲から除外した上で、広い意味で商業的価値が認められる情報を保護することに主眼がある。

（２）したがって、秘密管理性、非公知性要件を満たす情報は、有用性が認められることが通常であり、また、現に事業活動に使用・利用されていることを要するものではない。

同様に、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む。例えば、過去に失敗した研究データ（当該情報を利用して研究開発費用を節約できる）や、製品の欠陥情報（欠陥製品を検知するための精度の高いAI技術[10]を利用したソフトウェアの開発

[10] 「ＡＩ・データの利用に関する契約ガイドライン－ＡＩ編－（平成３０年６月）」（以

には重要な情報）等のいわゆるネガティブ・インフォメーションにも有用性は認められる。

（３）なお、当業者であれば、公知の情報を組み合わせることによって容易に当該営業秘密を作出することができる場合であっても、有用性が失われることはない（特許制度における「進歩性」概念とは無関係）。

４．非公知性の考え方

「非公知性」が認められるためには、一般的には知られておらず、又は容易に知ることができないことが必要である。

（１）「公然と知られていない」状態とは、当該営業秘密が一般的に知られた状態になっていない状態、又は容易に知ることができない状態である[11]。具体的には、当該情報が合理的な努力の範囲内で入手可能な刊行物に記載されていない、公開情報や一般に入手可能な商品等から容易に推測・分析されない等、保有者の管理下以外では一般的に入手できない状態である。

（２）営業秘密における非公知性要件は、発明の新規性の判断における「公然知られた発明」（特許法第２９条）の解釈と一致するわけではない。特許法の解釈では、特定の者しか当該情報を知らない場合であっても当該者に守秘義務がない場合は特許法上の公知となりうるが、営業秘密における非公知性では、特定の者が事実上秘密を維持していれば、なお非公知と考えることができる場合がある。また、保有者以外の第三者が同種の営業秘密を独立に開発した場合、当該第三者が秘密に管理していれば、なお非公知である。

（３）また、当該情報が実は外国の刊行物に過去に記載されていたような状況であっても、当該情報の管理地においてその事実が知られておらず、その取得に時間的・資金的に相当のコストを要する場合には、非公知性はなお認められうる。もちろん、そのようなコストを投じて第三者が現に当該営業秘密を取得又は開発した上で当該情報の管理地において公開等を行い、「公然と知られている」状態となれば、非公知性は喪失することになる。

下、「ＡＩガイドライン」という。）（http://www.meti.go.jp/press/2018/06/20180615001/20180615001-3.pdf）と同様に、本指針における「AI 技術」は、機械学習、又はそれに関連する一連のソフトウェア技術のいずれかを意味するものとする。なお、ＡＩガイドラインでは、「機械学習」は、「あるデータの中から一定の規則を発見し、その規則に基づいて未知のデータに対する推測・予測等を実現する学習手法の一つである。」と説明されている。

[11] ＴＲＩＰＳ協定 39 条 2 項（a）号も同様の要件を規定している。

（４）なお、「営業秘密」とは、様々な知見を組み合わせて一つの情報を構成していることが通常であるが、ある情報の断片が様々な刊行物に掲載されており、その断片を集めてきた場合、当該営業秘密たる情報に近い情報が再構成され得るからといって、そのことをもって直ちに非公知性が否定されるわけではない。なぜなら、その断片に反する情報等も複数あり得る中、どの情報をどう組み合わせるかといったこと自体に価値がある場合は、営業秘密たり得るからである。複数の情報の総体としての情報については、組み合わせの容易性、取得に要する時間や資金等のコスト等を考慮し、保有者の管理下以外で一般的に入手できるかどうかによって判断することになる[12]。

〈参考裁判例〉

（肯定例）

・仮に原告製品のリバースエンジニアリングによって原告の営業秘密である技術情報に近い情報を得ようとすれば、「専門家により、多額の費用をかけ、長時間にわたって分析することが必要である」と推認されることを理由に、非公知性を肯定（大阪地判平成 15 年 2 月 27 日　平成 13 年（ワ）10308 号）。

（否定例）

・一般的に利用可能な技術手段であって、その費用も過大ではない成分分析を用いて、市場で流通している原告製品に用いられている合金の種類や配合比率を調べることが容易であることを理由に、非公知性を否定（大阪地判平成 28 年 7 月 21 日　平成 26 年（ワ）第 11151 号、平成 25 年（ワ）第 13167 号）

12　例えば、公知情報を組み合わせて作成した AI 技術の開発（学習）用のデータについては、その組み合わせの容易性、取得に要する時間や資金等のコスト等を考慮して、その非公知性が判断されるものと考えられる。

おわりに

営業秘密は、我が国企業の競争力の源泉として、その重要性をますます増している。

一方で、その内容や管理方法は、情報の性質、ライバル企業との競争環境、従業員の多寡、グローバル展開の度合い、業務委託の状況、情報通信技術の進歩といった要素が複雑に影響し、企業によって極めて多様であり、絶えまない進化が求められる側面もある。

企業においては、本指針の趣旨を基礎としつつ、企業実態に即した、実効的な営業秘密管理に向けた創意工夫の発揮が期待される。

また、そのような創意工夫が、本指針を踏まえたものである限り、全ての関係者において最大限尊重され、結果として、営業秘密が保護・活用され、我が国の経済活力に寄与するようなナショナルシステムが実現することを期待したい。

営業秘密管理指針

発　行　　２００３年　１月３０日
　　２０１９年　１月２３日　最終改訂

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