

「営業秘密管理指針」の 主な改訂内容一覧

令和7年1月

経済産業省知的財産政策室

「営業秘密管理指針」改訂の背景・方向性

- 「営業秘密管理指針」の最終改訂が平成31年1月であり、近時の管理実態や平成31年・令和元年以降の裁判例の蓄積を踏まえ、さらなる明確化を図る必要性が生じている。

営業秘密をととりまく「環境の変化」に伴う修正（第26回不競防止小委員会資料5参照）

- 働く環境の変化（テレワークの普及、雇用の流動化）を踏まえた記載内容の整理・拡充（対従業員管理・対取引先管理の明記など）。
- 情報管理方法の変化（クラウド利用の普及）に伴う記載内容の整理・拡充。
- 技術動向を踏まえた営業秘密管理に関する記載の整理・追加（生成AIとの関係、リバースエンジニアリング、ダークウェブ）。

関連する法制度の見直し、裁判の動向を踏まえた修正

- 前回改訂以降の不正競争防止法改正の動向（平成30年の限定提供データ制度の導入、令和5年改正での営業秘密との関係の整理）、営業秘密に関連する裁判の動向を踏まえた記載の整理・拡充。
- 大学・研究機関も営業秘密の保有者になることの明示。

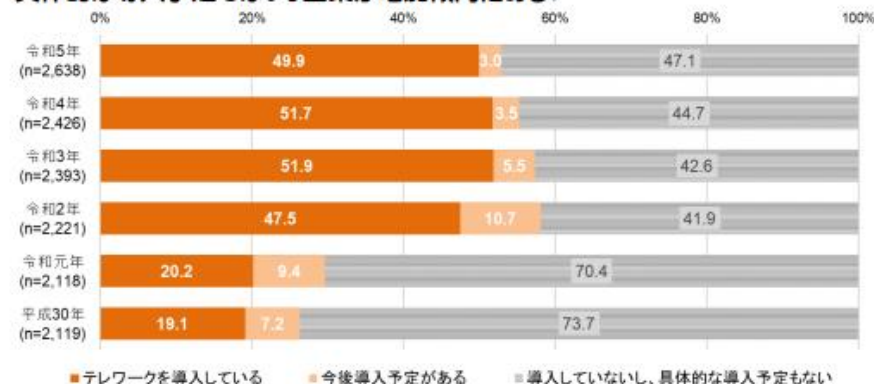
(参考) テレワークの導入状況等

4 テレワークの導入状況等(企業)

5

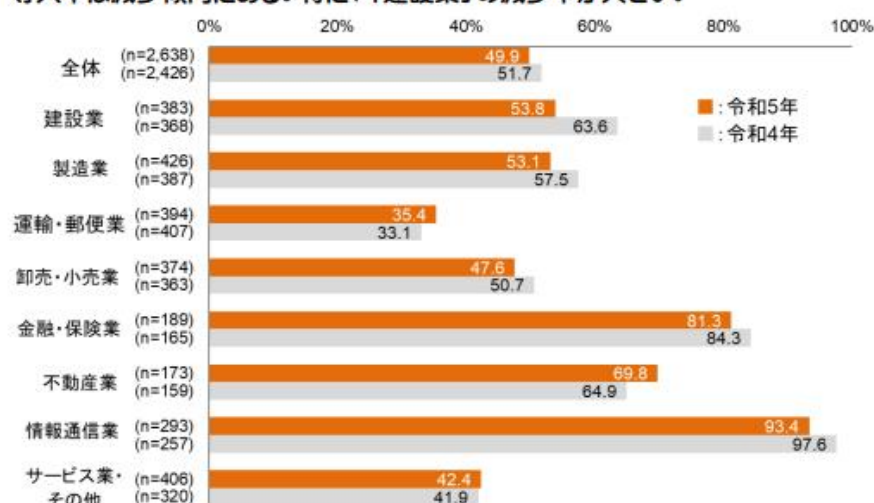
テレワークの導入状況

テレワークを導入している企業の割合は約5割となっており、「導入していないし、具体的な導入予定もない」企業が増加傾向にある。



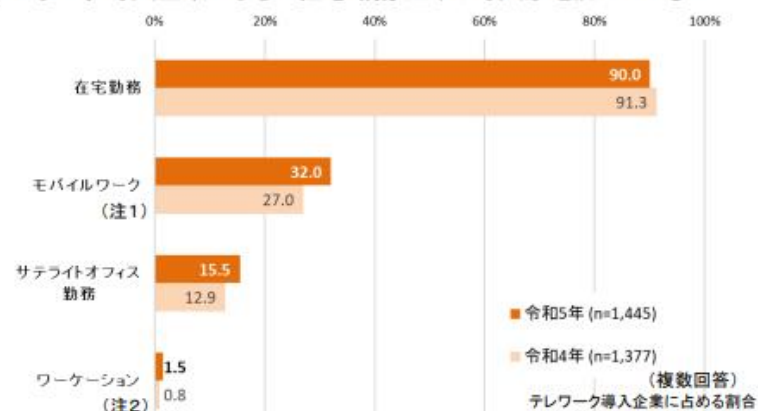
産業別テレワークの導入状況

「情報通信業」が9割以上、「金融・保険業」においても8割以上が導入しているが、導入率は減少傾向にある。特に、「建設業」の減少率が大きい。



テレワークの導入形態

テレワーク導入企業のうち、在宅勤務以外の導入が増加している。

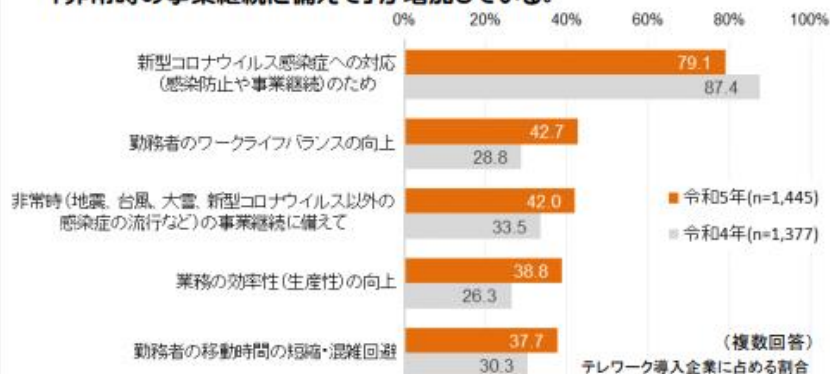


(注1) モバイルワークとは、営業活動などで外出中に作業する場合。移動中の交通機関やカフェでメールや日報作成などの業務を行う形態も含む。

(注2) ワケーションとは、テレワークなどを活用し、普段の職場や自宅とは異なる場所で仕事をしつつ、自分の時間も過ごすこと。

テレワークの導入目的

テレワークの導入目的は、「新型コロナウイルス感染症への対応」が前年より減少している一方、「勤務者のワークライフバランスの向上」、「非常時の事業継続に備えて」が増加している。



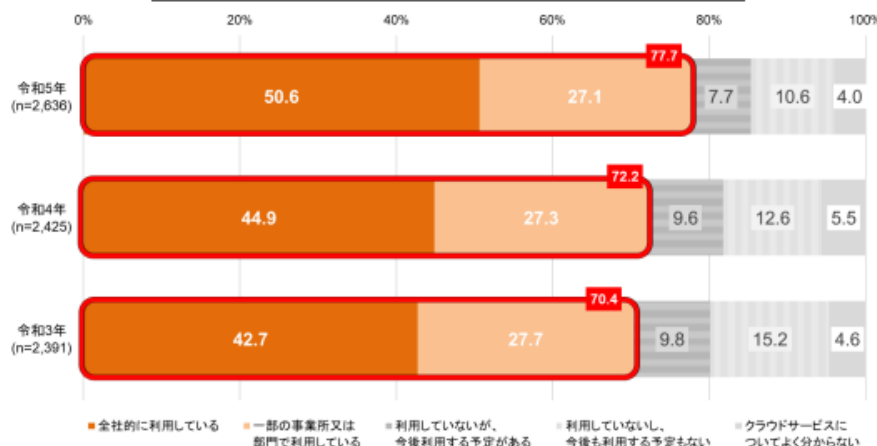
(参考) クラウドサービスの利用状況

5 クラウドサービスの利用状況(企業)

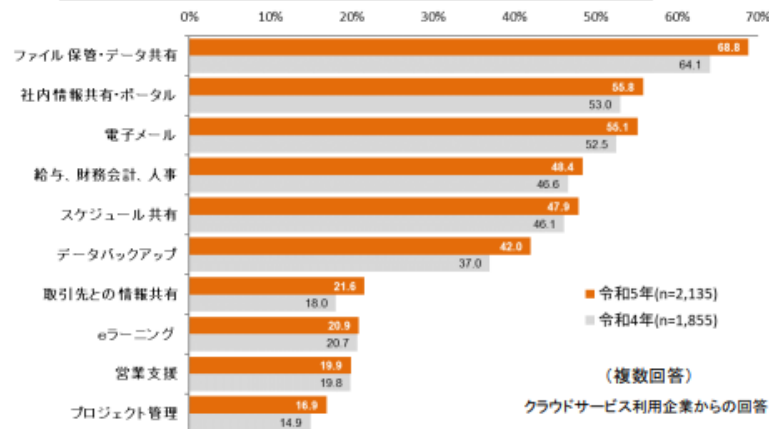
6

クラウドサービスを利用している企業の割合は上昇傾向が続いており、8割に近づいている。
利用用途は、「ファイル保管・データ共有」、「社内情報共有・ポータル」及び「電子メール」が5割を超えている。
利用する理由は、「場所、機器を選ばずに利用できるから」が、昨年から減少しつつも約5割となっている。
利用の効果については、利用企業の約9割が「非常に効果があった」又は「ある程度効果があった」と回答している。

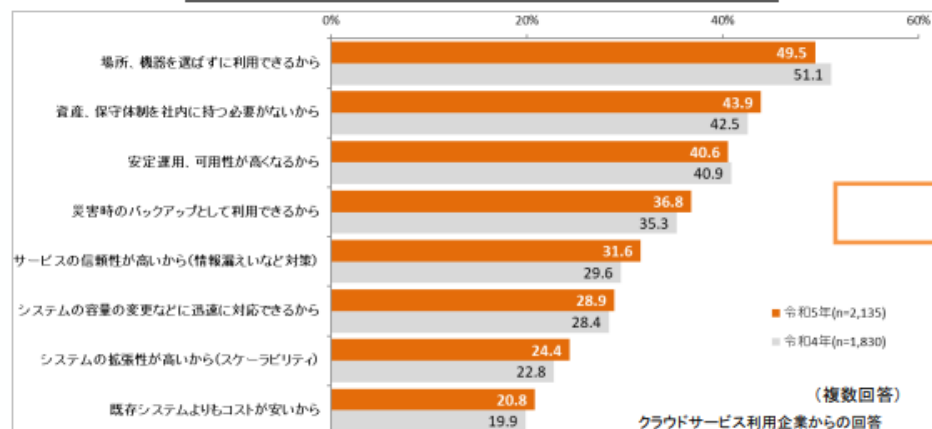
クラウドサービスの利用状況



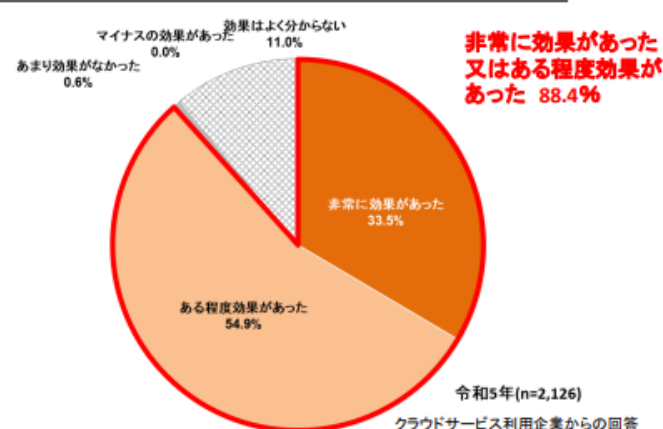
クラウドサービス利用の用途



クラウドサービスを利用する理由



クラウドサービス利用の効果



(参考) 「営業秘密管理指針」について

(<https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf>)

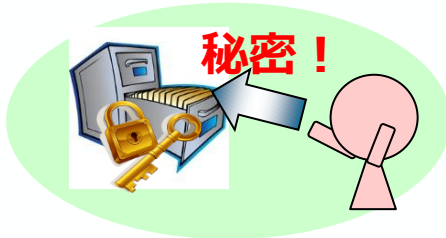
- 「営業秘密管理指針」とは、不正競争防止法により営業秘密として法的保護を受けるために必要となる「最低限の水準の対策」を示すことに特化したガイドライン。

<法的保護レベル>

営業秘密保有企業の秘密管理意思(※1)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**(※2)が確保される必要。(営業秘密管理指針p.5)

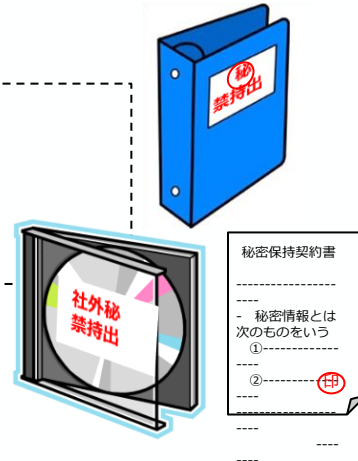
※1) 特定の情報を秘密として管理しようとする意思。※2) 情報にアクセスした者が秘密であると認識できること。

⇒情報に接することができる従業員等にとって、**<秘密だと分かる程度の措置の例>**
秘密だと分かる程度の措置



※企業、大学や研究機関の実態・規模等に
応じた合理的手段でよい

- 紙、電子記録媒体への「マル秘[®]表示」
- 化体物（金型など）のリスト化
- アクセス制限
- 秘密保持契約等による対象の特定



上記はあくまで例示であり、**認識可能性**がポイント。

秘密情報の
漏えい対策

営業秘密
管理指針

☞ 営業秘密管理指針で示されている「秘密管理性」の考え方は、秘密情報の漏えい対策にも共通。漏えい対策をしつつ、法的保護レベルの対策を確保することが大切。

(参考) 「営業秘密管理指針」の位置づけ・ 「秘密情報の保護ハンドブック」との関係

- 「営業秘密管理指針」は、不正競争防止法により「営業秘密」として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。(平成15年1月策定、27年1月全面改定、31年1月最終改訂)
- 「秘密情報の保護ハンドブック」は、企業が保有する「秘密情報」について、法的保護レベルを超えて、情報漏えい対策として有効と考えられる対策や推奨される対策等を包括的・網羅的に紹介するもの。(平成28年2月策定、令和6年2月最終改訂)

営業秘密管理指針について

- 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として平成27年1月に策定。
- その後、第四次産業革命を背景とした情報活用形態の多様化を踏まえて平成31年1月に改訂。

秘密情報の保護ハンドブックについて

- 法的保護レベルを超えて、情報漏えい対策として有効と考えられる対策や、漏えい時に推奨される対策等をできる限り収集して包括的に紹介するものとして平成28年に作成。
- より良い漏えい対策を講じたい企業の方々に、企業の実情に応じて対策を取捨選択したり、参考としていただけるよう、様々な対策を網羅的に掲載。
- 簡易版「秘密情報の保護ハンドブックのてびき」も公表。

秘密情報の保護ハンドブック

(漏えい防止レベル)

営業秘密管理指針

(法的保護レベル)

主な改訂内容：はじめに

- 平成30年不正競争防止法改正により導入された限定提供データの保護と営業秘密との関係を整理。
- 企業における営業秘密の管理実態等を踏まえ、今般の営業秘密管理指針の改訂の背景を記載。

改訂の経緯について

【はじめに】 (改訂の経緯)

- 加えて、令和元年7月には、限定提供データの保護に係る平成30年に改正された不正競争防止法が施行されるとともに、令和6年4月には、限定提供データの保護対象について営業秘密を除外とする令和5年に改正された不正競争防止法が施行されている。改正法の施行に先立ち、「限定提供データに関する指針」を令和6年2月に改訂している³。
- さらに、従来、労働の場は企業の施設内に限られることが多かったものの、昨今の情勢を反映して、多くの企業でテレワーク勤務が実施されるに至るなど、企業の施設外における労働の機会が増えており、これに伴い、自宅等において営業秘密に触れる機会が増えている。また、企業における労働の担い手についても、企業内の従業員だけでなく、企業と派遣元との契約に基づいて派遣されてくる派遣労働者が、営業秘密に接する機会も増えてきている。さらに、労働形態の多様化の流れの中で兼業・副業の動きも見られ、兼業先・副業先の営業秘密に接する機会が更に増している。一方で、情報管理の手法については、クラウド技術・環境を前提とした管理が進むなど、企業における情報管理のあり方も変化している。
これらの動きを踏まえ、修辭上の修正とともに、令和●年●月に本指針の一部が改訂された。

³ 「限定提供データに関する指針」は以下に掲載。

<https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31pd.pdf>

主な改訂内容：はじめに

- 本指針は「営業秘密として法的保護を受けるために必要となる最低限の水準」を示すものである点、他関連指針・ハンドブック等の関係性も含めて改めて整理。

指針で示す管理水準等について

【はじめに】

(指針で示す管理水準等)

○ (指針で示す管理水準等)

- ・ 本指針は、企業等が保有する多様な情報のうち、不正競争防止法によって営業秘密とし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。営業秘密以外に、いわゆる機微情報や個人情報等の関係法令により情報保有者において適正な管理が必要とされる情報を含めて、企業や大学等の研究機関が保有する情報全般についての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⁴。
- ・ また、不正競争防止法においては、平成30年改正により限定提供データの保護を導入しており、営業秘密と相互補完的に企業等が保有する情報・データの保護を図っているところ、限定提供データとしての保護については、「限定提供データに関する指針」に掲載されているので、あわせて参照されたい。

主な改訂内容：1. 総説

- ・ 裁判例等を踏まえ、民事上の措置・刑事罰との関係を明確化。
- ・ 営業秘密以外の情報の保護について、限定提供データに関する関係性も含めて整理。

営業秘密と民事措置・刑事罰との関係について

【1. 総説】 (営業秘密と民事措置・刑事罰との関係)

○営業秘密と民事上の措置・刑事罰との関係

- ・ 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の救済上措置や、刑事罰上の措置の対象になりうることとなる。
- ・ 秘密管理性等の三要件の解釈については、民事上の要件と刑事上の要件とは同じものと考えられる⁵。
- ・ もともと、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、差止め等の民事上の措置や刑事罰上の措置の対象となるためには、法に定められている「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。

⁵ 「刑事上の措置においても、営業秘密該当性の要件は、不正競争防止法の平成15年改正の経緯等に照らしても、民事上の要件と同じものと解される」名古屋地判令和4年3月18日 平成29年（わ）427号）

⁶ 営業秘密と同様に、限定提供データに該当したとしても、差止め等の民事上の措置の対象となるためには、法に定められている「不正競争」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11号～第16号）ことに留意する必要がある。

営業秘密以外での情報の保護について

【1. 総説】 (営業秘密以外での情報の保護)

○契約による営業秘密以外での情報の保護

- ・ 営業秘密に該当しない情報については、営業秘密としては法による保護を受けることはできないものの、同じ不正競争防止法に基づく限定提供データ（法第2条第7項）による保護や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可能性もある。
- ・ 例えばすなわち、当該情報が営業秘密に該当しない場合であって限定提供データに該当するときは、限定提供データに基づく差止め等を請求することが可能な場合もある⁶。
- ・ また、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な場合もあるが⁷、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。
- ・ さらに、当該情報が営業秘密や限定提供データに該当せず、また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なかった場合であっても、不法行為に該当し、損害賠償を請求することができる可能性もある。

主な改訂内容：1. 総説

- ・ 裁判例等を踏まえ、「事業者」の範囲について明確化。

本指針の対象となる「事業者」の範囲について

【1. 総説】

(本指針の対象となる「事業者」の範囲)

※新設

○本指針の対象となる「事業者」の範囲

- ・ 本指針では、「企業」、「従業員」などといった民間企業を念頭に置いた記載となっているが、その内容は大学・研究機関における営業秘密の管理・保護においても十分にあてはまるものである。
- ・ 貴重な研究成果は、大学・研究機関にとって民間企業におけるものと同様に秘密として価値を有しており、不正競争防止法が対象とする「営業秘密」に該当する情報となる⁷。このため、大学や研究機関が「営業秘密」を保有することは十分にあり得る。
- ・ 実際、不正競争防止法において、「事業者」として大学が対象に含まれることを前提とした裁判例も存在しており⁸、また、研究機関に勤務する研究員による営業秘密にあてはまるとされる情報の持ち出し（外部への漏えい）が、不正競争防止法違反として問題となった事例も起きている。よって、本指針における「事業者」の範囲として、大学・研究機関についても該当し得ると考えられる。

⁷ 大学や研究機関が保有する情報のうち、例えば共同研究の相手先の民間企業から提供を受けた外部の秘密情報だけでなく、大学や研究機関が生み出し、保有している研究・実験データなども不正競争防止法が対象とする「営業秘密」に該当する情報となる。

⁸ 東京地判平成13年7月19日判時1815号148頁

主な改訂内容：2. 秘密管理性について

- 総則における事業者の範囲の明確化を受けた修正や従業員等の定義を明確化。加えて、秘密管理措置の対象者の考え方を明確化。

秘密管理性要件の趣旨

【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、企業事業者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⁹や役員、取引相手先など（以下、「従業員等」という。）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。

⁹ ここでは、派遣先の指揮命令を受けて労働に従事するという観点から、「労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律」（いわゆる労働者派遣法）に基づく派遣労働者が含まれる。

秘密管理措置の対象者について

【2. 秘密管理性について】

（2）必要な秘密管理措置の程度 （秘密管理措置の対象者）

○（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、現実には接すること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。

なお、秘密管理性は、従業員全体の認識可能性も含めて客観的観点から定めるべきものであり、従業員個々が実際にどのような認識であったか否かに影響されるものではない¹³。

¹³ 知財高判令和3年6月24日 令和2年（ネ）10066号参照

主な改訂内容：2. 秘密管理性について

- 企業における管理実態を踏まえ、「秘密管理措置の程度」の中に、合理的区分を含めた考え方を入れ込むとともに、参考裁判例の追加を含め、対象事業者毎に注意すべき項目を整理。

合理的区分について

【2. 秘密管理性について】

(2) 必要な秘密管理措置の程度 (合理的区分)

※管理対象の整理（対従業員・対取引先）に伴い、記載位置・内容を整理

○（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¹²。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。~~

主な改訂内容：2. 秘密管理性について

秘密管理措置の程度について

【2. 秘密管理性について】

(2) 必要な秘密管理措置の程度 (秘密管理措置の程度)

○ (その他の秘密管理措置の程度)

ア 従業員及び役員に向けたもの

- 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、営業秘密と他の情報との分別管理ないし、営業秘密たる情報の種類・類型のリスト化、就業規則や秘密保持契約（あるいは誓約書）などの規程等において守秘義務を明らかにする、従業員への研修・啓発¹⁵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（管理措置）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（重要性）、執務室の状況その他の事情によって当然に異なる。
- 例えば、情報の性質に関して、当該営業秘密保有者にとって重要な情報であり、当然に秘密として管理しなければならないことが従業員にとって明らかな場合には、そうした従業員の認識を活用した管理が許されて然るべきであり¹⁶、IDやパスワードなどといった程度の技術的な管理措置や、就業規則や誓約書において当該情報の漏えいを禁止しているといった規範的な管理措置で足りる場合もある¹⁷。

➤ 当該媒体に接触する者の限定に関して、従業者ごとに厳密に業務の必要性を考慮した上で限定することまでは求められるものではなく、業務上の必要性等から特定の部署で広くアクセス権限が付与されていたとしても、特定の従業員に限定されていたことに変わりはないと考えられる¹⁸。

➤ 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。

(略)

・ また、情報セキュリティについては、企業が被る不利益を減らす観点から企業が置かれている状況毎に必要な措置を行うことが重要ではあるが、情報セキュリティで求められる措置の程度と秘密管理措置の程度は異なってもよく、情報セキュリティで求められる措置の程度に達していなくとも、秘密管理措置を認められ得る。

¹⁵ 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、状況に応じた具体的な管理方法等について、従業員に対する周知等が考えられる。

¹⁶ 知財高裁平成23年9月27日 平成22年（ネ）10039号、東京地判令和4年12月9日 令和3（特ワ）129号等参照

¹⁷ 大阪地判平成30年3月5日 平成28年（ワ）648号参照

¹⁸ 福岡高判令和6年7月3日 令和6年（ウ）20号参照

主な改訂内容：2. 秘密管理性について

秘密管理措置の程度について（続き）

【2. 秘密管理性について】

（2）必要な秘密管理措置の程度 （秘密管理措置の程度）

〈参考裁判例〉

（略）

・ 規範的な管理がなされていることに加え、情報の重要性に鑑みて従業員等が認識可能であると認定した例

アクセス制限の程度が明らかでなく、また物理的な管理が徹底されていたとはいいがたい事情があるとしても、顧客情報を一元化してデータ管理しており、就業規則において顧客情報の開示等を禁止することに加え、退職従業員に対しても、顧客情報を漏えいしないことを誓約させるなど、規範的な管理がなされていたことに加え、顧客情報の重要性に鑑みて、従業員らにとっても、それが秘密管理の対象とされるべきものであることは容易に理解し得るとして秘密管理性を肯定（大阪地判平成 30 年 3 月 5 日 平成 28 年（ワ）648 号）。

イ 取引相手先に向けたもの

- ・ 取引相手先に秘密情報を提供している場合には、従業員に向けた秘密管理措置に加えて、当該取引相手先と秘密保持契約を締結した上で秘密情報を提供したかどうかのポイントとなる。

主な改訂内容：2. 秘密管理性について

- 企業における管理実態を踏まえ、外部クラウド利用による秘密管理措置、生成AIの利活用に関する具体例を追記。

典型的な管理方法について

【2. 秘密管理性について】

(3) 秘密管理措置の具体例

①紙媒体の場合

- ~~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、基本的に例えばは、~~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他にも、~~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。

【2. 秘密管理性について】

(3) 秘密管理措置の具体例

②電子媒体の場合

- 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、情報の内容・性質等からいって、当該営業秘密保有者にとって重要な情報であることが明らかな場合には、外部クラウドにアクセスするためにID・パスワードなどが設定されているといった程度の技術的な管理措置や、就業規則や誓約書において当該情報の漏えいを禁止しているといった規範的な管理措置で足りる場合もある。

【2. 秘密管理性について】

(3) 秘密管理措置の具体例

④媒体が利用されない場合

- 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、民事上の措置上及び刑事罰上の措置の対象となるわけではない。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場合、すなわち「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、民事上の措置上又は刑事罰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~~²⁰。

主な改訂内容：2. 秘密管理性について

生成AIとの関係における秘密管理性の考え方

【2. 秘密管理性について】

(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

① 社内の複数箇所で同じ情報を保有しているケース

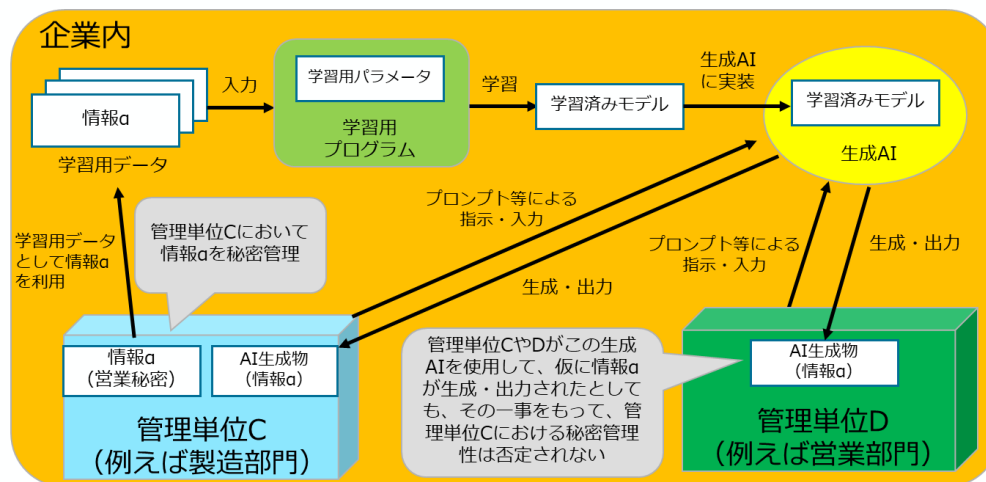
すなわち、管理単位（規模、物理的環境、業務内容も勘案しつつ、秘密管理措置の要否や内容の決定及びその遵守状況の監督（違反者の処分等）に関する自律的決定権限の有無その他の事情の有無から判断して、営業秘密の管理について一定の独立性を有すると考えられる単位。典型的には、「支店」「事業本部」など。）ごとに、当該企業の秘密管理意思に対する認識可能性があればよい。

※注1 十分な秘密管理措置が行われている管理単位A単位から情報が漏えいした場合において、管理単位B単位における秘密管理措置の不存在をもって、管理単位A単位の秘密管理性は通常、否定されない。ただし、管理単位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、管理単位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、管理単位A単位から情報が漏えいした場合ときに、管理単位A単位における秘密管理性は否定される（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）。

※注2 生成AIにおける学習用データとして情報αを利用していた場合において、その後、管理単位Cにおいて当該情報αが生成・出力されることがあったとしても、当該情報αが管理単位Cにおいて秘密管理されているのであれば、当該情報αが生成・出力されたことの一事をもって、管理単位Cにおける秘密管理性が否定されることはないと考えられる²¹。また、管理単位Cにおいて秘密管理していた当該情報αが、管理単位Cではなく管理単位Dにおいて生成・出力された場合でも当該情報αが管理単位Cにおいて秘密管理されているのであれば、当該情報αが生成・出力されたことの一事をもって、管理単位Cにおける秘密管理性が否定されることはない。

²¹ ただし、当該企業にとどまらず、当該情報αが当該企業以外の第三者に提供される場合は、秘密管理性が否定される場合もあり得る。

【参考例】



※生成AIは当該企業内でしか使用できない前提

主な改訂内容：3. 有用性の考え方

- 昨今の裁判例を踏まえ、当該情報を取得した者の認識に関わらず、事業者の事業活動に利用されているのであれば、有用性の要件が充足されるものであると考えられる旨等を追記。

有用性要件の充足について

【3. 有用性の考え方】 (2)

(2) したがって、当該情報が、営業秘密を保有する事業者の事業活動に使用・利用されているのであれば、基本的に営業秘密としての保護の必要性を肯定でき、当該情報が公序良俗に反するなど保護の相当性を欠くような場合でない限り有用性の要件は充足されるものと考えられる²²。

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、また加えて、必ずしも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²³を利用したソフトウェアの開発には重要な情報）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。

²² 東京地判令和4年12月9日 令和3年（特わ）129号、東京地判令和6年2月26日 令和4年（特わ）2148号参照

有用性要件の判断について

【3. 有用性の考え方】 (3)

(3) なお、有用性の要件の判断に際しては、当該情報を取得した者がそれを有効に活用できるかどうかにより左右されない²⁴。

また、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）²⁵。

〈参考裁判例〉

・「不正競争防止法が営業秘密を保護する趣旨は、不正な競争を防止し、競争秩序を維持するため、正当に保有する情報によって占め得る競争上の有利な地位を保護することにある、進歩性のある特別な情報を保護することにあるとはいえないから、当該情報が有用な技術上の情報といえるためには、必ずしもそれが「予想外の特別に優れた作用効果」を生じさせるものである必要はないというべきである。」（横浜地判令和3年7月7日 平成30年（わ）1931号等）。

²⁴ 東京地判令和4年12月9日 令和3年（特わ）129号、東京地判令和6年2月26日 令和4年（特わ）2148号参照

²⁵ 横浜地判令和3年7月7日 平成30年（わ）1931号等参照

主な改訂内容：4. 非公知性の考え方

- 昨今の裁判例等を踏まえ、ダークウェブ、AI学習用データを想定した公知情報の組み合わせ、進歩性の議論、リバースエンジニアリング等について追記。

ダークウェブに公表された場合について

【4. 非公知の考え方】

(ダークウェブに公表された場合)

※新設

○(ダークウェブに公表された場合)

- ・ 第三者からのハッキング等により営業秘密が、ダークウェブ²⁸に公表されたとしても、その一事をもって直ちに非公知性が喪失するわけではない。

²⁸ ここでいうダークウェブとは、一般的な方法ではアクセスできず、また検索エンジンで見つけることも不可能な Web サイトの総称を指す。

公知情報の組み合わせについて

【4. 非公知の考え方】

(公知情報の組み合わせ)

○(公知情報の組み合わせ)

- ・ —(4)—なお、「営業秘密」とは、様々な知見を組み合わせる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²⁹。例えば、公知情報の組み合わせであっても、その組み合わせが知られていなかったり容易に知り得ないため、財産的価値が失われていない場合には非公知と云いうる。また、仮に公知情報の組み合わせであっても、その組み合わせが知られていたり容易であったりしたとしても³⁰、取得に要する時間や資金的コストがかかるため財産的価値があるという場合には非公知と云いうる。

²⁹ 名古屋地判令和4年3月18日 平成29年(わ)第427号参照。

³⁰ 公知情報を組み合わせで作成したAI技術の開発(学習)用のデータのようなものが想定される。

主な改訂内容：４．非公知性の考え方

特許法の進歩性との関係について

【４．非公知の考え方】 (進歩性（特許法第２９条第２項）との関係) ※新設

○（進歩性（特許法第２９条第２項）との関係）

- ・ 不正競争防止法が営業秘密を保護する趣旨は、進歩性のある特別な情報を保護することにあるのではないから、当該情報が非公知の情報といえるための要件として「予想外の特別に優れた作用効果」を生じさせるものであることまでは要しない³¹。

³¹ 東京高判令和４年２月１７日 令和３年(う)1407号参照

リバースエンジニアリングについて

【４．非公知の考え方】 (リバースエンジニアリング) ※新設

○（リバースエンジニアリング）

- ・ リバースエンジニアリング³²によって営業秘密を抽出できる場合、抽出可能性の難易度の差によって判断がわかれることになる。具体的には、誰でもごく簡単に製品を解析することによって営業秘密を取得できるような場合には、当該製品を市販したことによって営業秘密自体を公開したに等しいと考えられることから、非公知性を喪失すると考えられる。これに対し、特殊な技術をもって相当な期間が必要であり、誰でも容易に当該営業秘密を知ることができない場合には、当該製品を市販したことをもって非公知性を喪失するとはならない。

³² ここでいうリバースエンジニアリングとは、製品を解析、評価することによって、その構造・材質・成分・製法等その製品に化体している情報を抽出したり、抽出した情報を使用する行為を意味する。