

第2章 保有する情報の把握・評価、秘密情報の決定

- ・ 企業が保有する情報は、その一つ一つの情報ごとに、その経済的な価値や漏えいしたときに生ずる損失、情報の性質等が異なります。
- ・ その違いを踏まえずに、闇雲に情報管理策を実施してしまうと、費用と手間がかさむ割には情報漏えい防止の効果が乏しくなったり、本当に必要なときに情報を利用できなくなるなど、業務効率の低下につながったりするおそれもあります。いたずらに秘密情報の対象範囲が広がることによって、かえって、真に重要な情報をいざというときに守ることができないという状況も招きかねません。
- ・ また、企業が保有する情報の中には、特許権などの権利を取得することによって、法的保護の下で公開しつつ活用すべきものや、個人情報のように外部への漏えいは一切許してはならない情報もあります。よって、自社が保有する情報のうち、どの情報を公開し、どの情報を秘密情報とするのかを、自らの意思を持って適切に判断して組み合わせ、収益の最大化を図っていく必要があります。
- ・ 本章では、まず自社が保有する情報全体を把握した上で、その評価を行い、それらの情報の中から秘密情報を決定するというステップ（図表1（1）で示したステップ1）の具体的方法について、順を追って紹介します。

（本章で紹介する方法について）

- 本章では、これから初めて秘密情報の管理を開始しようとしている企業を念頭に、自社が保有する情報⁴から秘密情報を決定するまでのステップを紹介しています。一方で、本書を参照する企業の中には、既に、保有する情報の全体像の把握、その評価、秘密情報の決定、秘密情報の取扱いに関する社内規程の整備など、取組みがある程度進んでいる企業も存在すると考えられます。
- そのような場合には、本章で示す手順にこだわらず、自社の取組みの進捗状況に応じて、例えば、
 - ・ 2-2で示す観点を参考としながら、秘密情報とすべき情報に不足がないかどうかの検証として、漏えいした場合に甚大な悪影響がある、いわば「虎の子の情報」や「独自のノウハウ」等を、部署ごとに探し出し、それを報告させる
 - ・ 本章で示す評価・秘密情報の決定に係る観点を参考としながら、社内規程に

⁴ ここでいう「自社が保有する情報」とは、事実上自社内に存在するあらゆる情報を対象としています。

基づき既に各部署において実施している秘密情報の指定が適切に行われているか否か、その社内規程自体が適切な内容となっているか否かなどを確認する

といった形で、本章で紹介する方法を参照いただくことが考えられます。どのような形であれ、自社が保有する情報の全体像が把握され、それらが適切に評価された上で、秘密情報とすべき情報が適切に決定されている状況となっていることが重要です。

2-1 企業が保有する情報の評価

(1) 企業が保有する情報の全体像の把握

- 秘密情報の管理のファーストステップは、自社の保有する情報を把握して、経済的価値や漏えい時の損失の程度といった指標に基づいて評価することです。このステップを通じて、企業は、単に秘密情報を決定するだけでなく、自社の持つ強みやその源泉を再確認して、今後の更なる競争力強化の可能性の検討につなげることができます。

(企業が保有する情報とは)

- まずは、自社において「どういった情報を保有しているのか」を全体的に把握することから始まります。その際、情報は、紙に記載されていたり、サーバーやPC、USBメモリ等の機器・媒体に記録された電子データ等のような形で存在するだけではありません。その他にも、従業員が業務の中で記憶した製造ノウハウなど文章化されず目に見えない形で存在する場合や、プラントのレイアウト、金型、試作品などの「物」自体が把握すべき情報である場合もあるので留意する必要があります。こうした情報も含めて、自社が保有する情報を把握することは、秘密情報の管理の一環であるだけでなく、自社の財産としての情報資産を認識することでもあり、これまで活用されていなかった情報資産を社内で共有・活用することの促進にもつながります。
- なお、個々の企業における製品やサービスが変化するなど、企業活動、そしてそれを取り巻く環境は常に変化し、それに伴い技術情報や顧客情報、取引情報などの企業が取り扱う情報の種類や重要性も変化することがあります。したがって、必要に応じてその変化に対応した追加的な情報の把握や更新をすることも重要です。

（保有する情報の把握方法）

- 保有する情報の把握に当たっては、個別の担当者の感覚によって、その判断にばらつきが生じないようにするため、事業規模や扱う情報の多寡等に応じて、社内で統一的な判断が可能となるような情報の把握方法を取ることが望ましいでしょう。例えば、具体的方法としては、以下のような方法が考えられます⁵。
 - ① 経営者等の責任者が社内の各部署や担当者に対して直接ヒアリング等を実施することにより把握する方法
 - ② 秘密情報の管理を統括する部署が統一的な基準を示しつつサポートしながら、各部署や個別の担当者に、その基準に則してそれぞれが有する情報を経営者等の責任者に報告させ、情報を集約することにより把握する方法

- なお、自社が保有する情報を把握する際に、特に他社との差別化要因となっている（自社の強みとなっている）情報を漏れなく把握するためには、競合他社との製品・サービス等の差異を分析することが有効です。例えば、他社と比較して個性が強い製品やサービス、高い売上げに結びつく特徴的な性質を持つものをピックアップし、その個性や特徴を生み出している要因を分析することで、自社が把握すべき情報が見えてくるでしょう⁶。従業員が業務の中で記憶した製造ノウハウなど文章化されず目に見えない形の情報、プラントのレイアウトや試作品などの「物」自体の情報については、紙媒体や電子データ等の形の情報に比べて、その把握が難しい場合が多いと考えられるため、特にこのような考え方が有効です。

（把握に当たっての留意点）

- 保有する情報の全体像の把握といっても、自社内に現在存在する書類や電子データ等の一つ一つを網羅的に確認するというものではありません。「○△製品の設計内容に係る情報」など、情報の種類を、一定程度、一般化・抽象化した形で把握することが必要となります。そのように把握することで、日々の業務の中、新たに生成されたり、入手したり、不要になるといった情報のライフサイクル等に伴い、常に変動する情報の全体像や取り扱う情報を適切に把握でき、後述の対策も立てやすくなります。

⁵ 社内の一定の技術情報については、各部署が全社共通の技術情報データベースに登録するシステムとしておくなど、情報の把握に資する取組みを日々の業務に組み入れるといった方法も考えられます。

⁶ 例えば、自社の主力製品が高い売上げを達成している理由として、その製品等が高い技術水準を有しているために他社の製品等と比べて競争力がある場合は、まずその技術自体が「自社の強み」といえ、その技術水準の実現を基礎付けている「製造ライン情報」、「人材育成プログラム」、「報酬体系情報」なども「自社の強み」と判断できます。

- そして、その一般化・抽象化した形での情報の把握に当たっては、その後の情報の評価や分類といった作業を見据えて、情報にアクセスできる者の範囲や、重要度の大きく異なる情報が混在することのない一般化・抽象化の程度について、一定程度念頭に置いた上で行うことが望ましいでしょう。

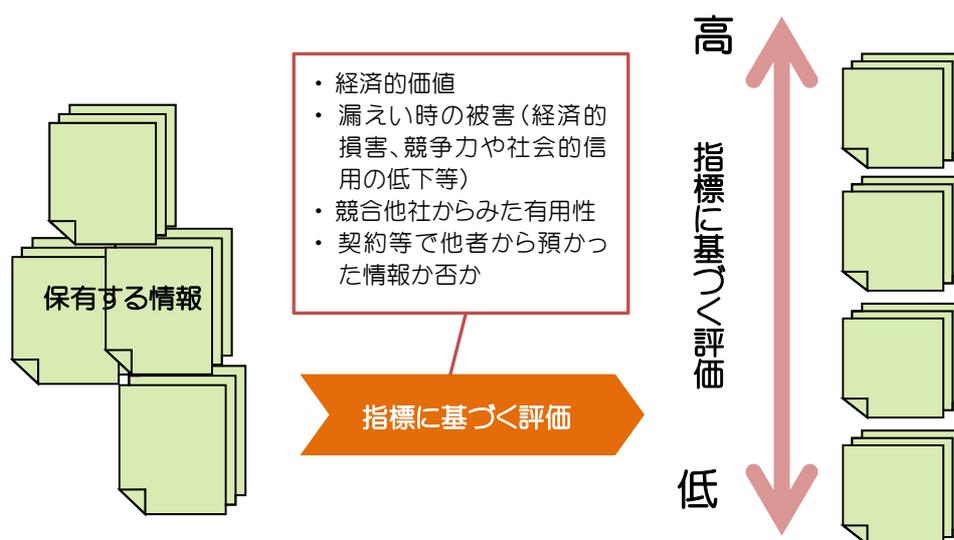
(良い例) ○△製品の設計内容に係る情報

(悪い例) ○△業務に関する情報・・・情報の対象範囲が広すぎて具体的でないため、アクセス範囲を限定すべき非常に重要な情報と、アクセスを特に限定しなくてもよい一般情報が混在してしまいます。その結果、この後の情報の評価や分類が適切になされないおそれがあります。

(2) 保有する情報の評価

- 次に、前述(1)の作業で把握した情報について、情報が生み出す経済的価値、他社に利用されたり漏えいしてしまった場合の自社の損失の大きさ(どの程度競争力や社会的信用が低下してしまうのか等⁷⁾、競合他社にとって有用か否か、悪用されるような性格の情報か否か、契約等に基づき他社から預かった情報が否か等、以下の観点を参考に評価を行い、その評価結果に応じて情報を階層化します。なお、本書は秘密情報の保護を目的としていますので、ここで実施する評価の対象は非公表の情報や未公開の情報等を前提としています。

図表2 (1) 評価のイメージ



⁷ 取引先の情報や顧客情報などについては、その漏えいによって、自社に対して損害賠償請求がなされる場合も考えられます。

【評価に当たって考慮すべき観点の例】

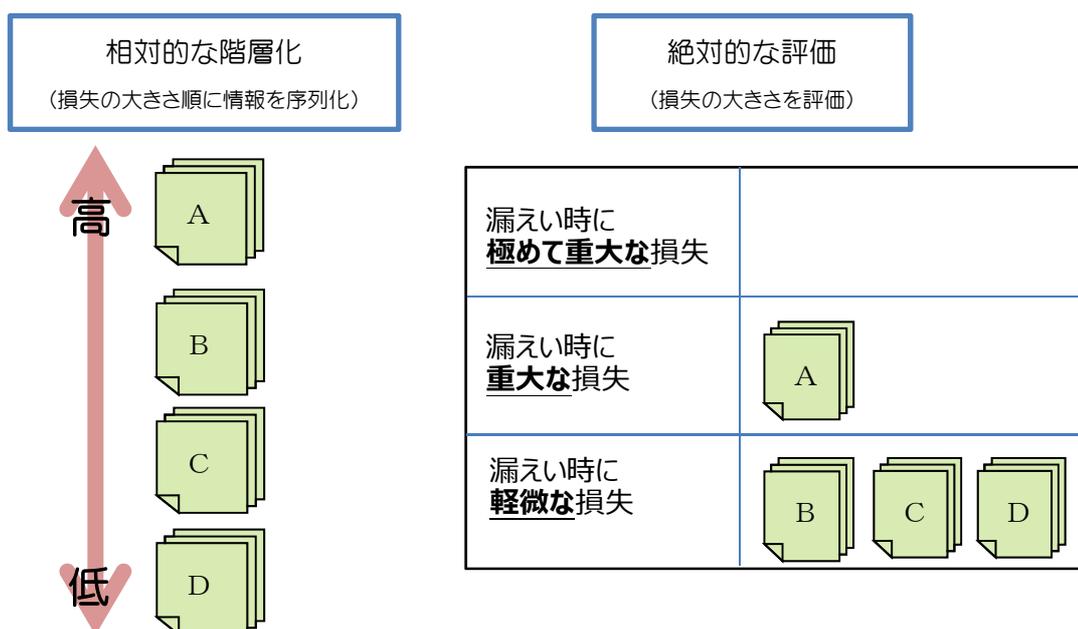
- 情報の経済的価値（その情報によって生み出される現在の価値、及びその分野における技術革新のスピードや代替技術の有無等を加味した将来的な価値）
- 情報漏えい行為等によって被る損失の程度
- 取引先など他社に与える損失の程度（例えば、情報が漏えいした場合、その情報を使用して製造した部品を納めた取引先に生ずる損失の程度）
- 競合他社にとっての有用性（情報が他社に渡った場合の他社のコスト削減及び他社製品の価格などへの影響の程度）
- 情報漏えい時の社会的信用低下（顧客減少等）による損失の程度
- 情報漏えい時の契約違反や法令違反に基づく制裁の程度

等

※第3章において、同様の対策を講ずるものごとに秘密情報を分類することを見据えて、ここでは、評価の高低によって、情報を相対的に階層化することに主眼を置いています。しかし、自社の対策全体としてどの程度厳格な対策を講ずるかを判断するためには、それぞれの情報が漏えいした際の実際の損失の程度等を念頭に置いておく必要があります。そのため、情報の相対的な階層化に加えて、その情報が絶対的にどの程度の評価がなされるものかを意識しておくことも重要です（例えば、自社の情報のうち最も評価の高いものであっても、漏えいしたときの損失がそれほど大きくないという場合には、全体としてそれほど厳格な対策を講じなくても良い場合もあり得ます）。

図表2（2）相対的な階層化と絶対的な評価のイメージ

—情報を損失で評価した場合—



- 前述（１）（２）の作業により、自社が保有する情報にはどのようなものがあるのか、そのうち自社の競争力の源泉となるような価値の高い情報は何かを認識（再認識）することができます。価値の高い情報を「見える化」して自社の財産として位置づけられれば、今後の事業展開に役立てることができます。

2-2 秘密情報の決定

- 次に、それぞれの情報の評価の高低を基準に、保護に値するものかどうかを判断します。保護に値するものであっても、その情報をより効果的に活用するための方法を、情報の性格に照らして検討することが重要です。
- 技術情報については、特許権など権利化して他社にライセンス⁸を行ったり標準化を行うことを通じて、他社にも自社技術を広く使用させ自社技術の市場を拡大させるという活用方法もある一方で、他社との差別化を図るために情報を独占することによって、自社の技術的優位性を高めるといった活用方法もあります。自社で独占する場合については、権利化した上で独占使用する方法や秘密として保持する方法が考えられますが、権利化する場合は情報が公開されることとなりますので、情報の性質なども考慮し、その情報の価値が最大限高められる活用方法を慎重に選択することが重要です。
- 顧客情報については、権利化、標準化の対象とならない性格のものでもあり、秘密として保持する方が適切と考えられます。
- 保護を要するものかどうかを判断する際には、想定される管理コスト、訴訟コスト（証拠収集等のための労力、費用、訴訟期間等）等のコスト、漏えいによって被るおそれのある損失、保護により得られる利益（損害賠償請求や侵害差止請求により取り戻すことが容易か否か）の総合考慮という観点から保護する意義がどの程度あるか、法令や他社との契約による特別の管理を求められる情報か否かという視点での判断が必要となる場合もあると考えられます。
- そのなかで、秘密として保持することを決定した情報が、自社の秘密情報となります。

⁸ 他社へのライセンスについては、権利化しないノウハウが対象となる場合もあります。

- 以下では、真に秘密として保持すべき情報を判断し、自社の秘密情報を決定する際に参考となる観点を紹介します。

(1) 秘密情報の決定に当たって考慮すべき観点のイメージ

①営業情報

- 自社独自の情報であり、それが漏えいした場合、自社の競争力が低下する情報か否か
(取引価格や取引先に関する情報、接客マニュアル、公表前のデザイン 等)
- その漏えいにより、法令違反や他社との契約違反等となり、自社の社会的信用の低下を招いたり、他社との信頼関係を毀損させる情報か否か
(顧客の個人情報、受託やライセンス等の他社との契約等により限定的に開示された営業情報 等)

②技術情報

- 市場に流通する自社の製品等を分析することによって容易にその製品に用いられている技術が判明してしまい、他社がすぐに追いつくことができる技術に関する情報か否か
→ 容易に判明する情報であれば、特許権などの知的財産権として権利化した方が活用しやすい可能性があります。
(部品の組合せ方法、新規素材の成分 等)
- 権利化した場合であっても、権利侵害の探知や立証が難しい情報か否か
→ 権利侵害の探知等が難しいものは、権利化のコストに見合う権利行使ができない可能性があるため、秘密情報とする方が良い可能性があります。
(製造ノウハウ 等)
- その漏えいにより、法令違反や他社との契約違反等となり、当該他社との信頼関係を毀損させる情報か否か
(受託やライセンス等の他社との契約等により限定的に開示された技術情報 等)
- 通信技術や試験方法などの社会基盤や技術標準となる技術であり、自社利益の最大化のためには当該技術の市場の拡大が求められる情報か否か
→ 将来的な市場拡大が見込めるので、秘密情報とするのではなく、権利化・

標準化した方が良い可能性があります。

※権利化する場合であっても、出願公開までは一定期間秘密情報とすべき場合や、権利化する技術実施に当たってのノウハウは秘密情報とすべき場合もあります。

※情報の評価の結果、情報漏えいの際の損失がほぼ生じず、侵害企業との訴訟に係る費用や管理コストのほうが確実に被害額を上回ると考えられる場合には、その情報については、積極的に公開しないものの、コストをかけて秘密として保持するための対策は行わないこともあり得ます。

- 以上の観点等により検証した結果、秘密として保持すべきと判断される情報を自社における秘密情報として決定し、第3章における情報漏えい対策の対象とします。