第４章　秘密情報の管理に係る社内体制のあり方

- 秘密情報漏えいの対策の実施（第２章、第３章）や、他社の秘密情報に係る紛争への備え（第５章）、秘密情報の漏えい事案への対応（第６章）といった、本書で紹介する取組み全般を、真に実効的なものとするためには、それらの対策が一時的なものとならないようにする必要があります。
- そのためには、秘密情報の管理の実施状況を定期的にチェックするとともに、状況の変化に応じた見直しを行うことができる社内体制を整えることが重要です。
- 秘密情報の漏えい対策に取り組む企業は、規模も業種も様々であることから、本章では、そのような社内体制の整備における基本的な考え方を示しつつ、考えられる社内体制の参考例を提示しています。

４－１　社内体制構築に当たっての基本的な考え方

（経営層の関与の必要性）

○ 秘密情報の管理は一旦対策を講ずれば完結するというものではなく、それが継続して実施され、状況の変化に応じて適切に見直しが行われるようにしていかなければなりません。

○ 秘密情報の管理に割くことができる費用や人員が限られている中で、網羅的な対策を実施することが困難である場合は、必ずしもその全てを実施しなければならないというものでもありません。守るべき情報の種類や企業規模等を踏まえて、適切と考えられる対策を選択して実施していくことが重要です。

○ いかなる対策を選択するかは、どの秘密情報が自社の経営戦略上重要性が高いのか、どの程度の費用・人員を割いて対策を実施するかといった経営判断によるべき問題であり、個々の部門で独自に判断することが望ましくない場合が多いと考えられます。

○ また、秘密情報は全ての部門に存在することが考えられ、かつ、その漏えい対策は、知的財産、人事・労務、情報セキュリティ、法務などの多様な観点からの対策を必要とすることから、自社内の個々の部門が、それぞれ独自に対策を行い、全体としての調整を欠いたままでは十分な対策を講ずることはできません。情報管理規程等の社内ルールの整備など、本来的に全社的に検討しなければならない対策も存在します。

○ 加えて、秘密情報の漏えいが、その情報の経済的な価値を失わせるのみならず、社会的信用の低下や他社からの訴訟リスクなど、様々な損失を生じさせるおそれがあることを踏まえると、コンプライアンスの観点からも、経営層が、率先して社内体制の構築に関与していくという意識を持つ必要があるでしょう。したがって、経営層が、自社内外に向けて、秘密情報の管理に取り組む姿勢（ポリシー）を明確に示し、自社内の個々人すべてが、秘密情報の管理の当事者であるという意識を持って、継続的に対策を講ずることができる体制を整えることが重要となります。

○ どのような社内体制が望ましいのかは、事業の規模や性質によって異なりますが、経営層の積極的な関与の下、以下の例を参考に、体制が単に形式的なものにならないように留意しながら、秘密情報の管理が継続的に実施され、状況の変化に応じた適切な見直しを行うことができる体制とすることがポイントです。

（小規模な企業における社内体制の具体例）

○ 小規模な企業であれば、以下のように特別の組織や会議体を設置するという形での体制整備よりも、例えば、

・　定例の社内会議等において、経営層も含めた全社員により、秘密情報の管理の実施状況の報告・確認や見直しを行う

・　社内において情報漏えい防止のために「これだけはやってはいけない」というような最低限の禁止事項を定め、周知徹底するとともにその実施状況を確認する

というような柔軟な体制のほうが、より実効的かつ効率的となる場合もあり得ます[40]。

[40] 特定個人情報の取扱いに関しては、『特定個人情報の適正な取扱いに関するガイドライン（事業者編）』（特定個人情報保護委員会）ｐ４７以下において、中小規模事業者における対応方法等が記載されています。（http://www.ppc.go.jp/files/pdf/261211guideline2.pdf）

小規模な企業における社内体制

◆　**金型製造業･小規模企業の事例**
～従業員全員で話し合い、当事者意識も向上～

従業員が十数名であることから、定期的に、社長も含めた全従業員で、秘密情報の管理に関する研究会を行っている。その研究会において、社内ルールの内容や運用の改善などについて議論し、現場の実情に即応した取組の見直しや取組の徹底を可能とするとともに、個々の従業員の当事者意識の向上にもつながっている。

◆　**工場設備製造業･小規模企業の事例**
～社長が責任者として見回り、情報管理を徹底～

従業員が20名程度と小規模であることから、あまり詳細なルールは策定していないが、社長が情報管理の責任者として、本社･工場を含めた3拠点に頻繁に足を運び状況確認を行うことで、情報管理の徹底を図っている。

（事業規模が大きな企業における社内体制の具体例）

○　**事業の規模が大きくなると、より組織的な体制を整えておく必要が生ずることから、例えば、担当取締役を決定の上、当該取締役を長として、秘密情報の管理の実施についてリーダーシップを取る部門横断的な組織を設置することが考えられます。（以下、部門横断的な組織について、便宜上「秘密情報管理委員会」という。）秘密情報の管理に係る判断は、重要な経営判断と密接に関連する場合もあるほか、仮に情報漏えいが起こった場合には会社としての迅速な判断が求められることから、そのような判断が円滑に、かつ適切に行われるようにするため、日頃からの取締役の関与が必要となるからです。**

※必ずしも「秘密情報管理委員会」を新たに設置する必要はなく、情報資産の管理を統括する「情報セキュリティ委員会」や、様々な経営リスクを管理することを目的とした「リスク管理委員会」、法令等の遵守一般を担当する「コンプライアンス委員会」といった社内に既に存在している別の組織に、同様の機能を担わせることも考えられます。

○　**また、「秘密情報管理委員会」は、経営企画、総務、法務、情報システム、営業、技術、製造、人事・労務、経理、知的財産など、情報漏えい対策に関連し得る社**

内の部門を広く巻き込む形で、各部門の責任者をもって構成することが望まれます（特に、「情報漏えい対策」とは関連性が薄いとの誤解がなされやすい人事・労務部門が抜け落ちないように留意）。加えて、「秘密情報管理委員会」の下に事務局を設置し、様々な社内規程案の作成や、部門間調整、「秘密情報管理委員会」の運営などの業務を担わせます。

○　なお、秘密情報管理委員会の運営にあたる事務局には、自社の経営戦略、ガバナンス、複数部門にわたるマネジメントなど多岐にわたる機能が求められます。よって、担当の取締役が、トップマネジメントとして、事務局に配属させるのに適切な人材を任命することも考えられます（必要に応じて、専門知識を有する者を参画させることも考えられます）。

（部門横断的な組織と各部門の役割分担）

○　一方で、事業規模が大きくなるにつれて、全社的に情報を集約して統一的に対策を検討し、その徹底を図ることや、適切な対策の見直しが困難になってくる場合もあります。そのような場合には、例えば、

・　全社的には基本的な方針のみを決定し、それ以外の秘密情報の管理の一部について、相当の規模の部門単位（例えば、２０～３０人程度の規模）に権限を降ろすという対応

・　相当の規模の部門単位ごとに、所属する部門単位（特に、営業、技術、製造部門）における秘密情報の管理の推進を担う責任者を任命し、その責任者を通じて、秘密情報の指定や分類の決定、対策の実施などの秘密情報の管理を徹底させるという対応[41]

など、事業規模等の各社の状況に応じて、部門横断的な組織と、各部門において、適切な役割分担を行うことがあり得ます。ただし、その場合でも、どの程度まで各部門に権限や責任を降ろすか等については、全社的な秘密情報の管理にばらつきが生じることのないように慎重に検討すべきでしょう。

【「秘密情報管理委員会」が担う役割（全社統一的に実施すべき対策）】

➢　社内規程の整備・見直し

秘密情報の管理方法等に関して社内においてルール化しておくべきことを社内規程とします。（参考資料２「第２　情報管理規程の例」を参照）

41　この対応の一環として、例えば、部門横断的に一定期間発足するプロジェクトの推進に当たって、そのプロジェクト独自で、秘密情報の管理の責任者の任命・対策の実施を行うことも考えられます。

例えば、

- 第２章で紹介した「保有情報の評価及び秘密情報の決定」及び第３章で紹介した「秘密情報の分類、情報漏えい対策の選択」を実施し、その内容をルール化
- 第３章で紹介した対策のうち、「アクセス権の範囲の適切な設定」や「秘密情報の表示」、「社外持ち出しルールや廃棄方法等のルール化」など、特に社内ルール化しておくべき対策のルール化

などを実施します。

- なお、ルール化にあたっては、必ずしも秘密情報の管理に係る独立したルールでなくとも良く、その他の保有情報を含めた情報管理全体のルールや、諸々のリスク対応に係るルールと統合された形も考えられます。

➢　各部門の役割分担の決定

第３章において選択した「情報漏えい対策」や第６章において紹介する事後対応に係る対応等について、自社内のどの部門に、どのような対策を担わせるかを決定します。対策の中には、サイバーセキュリティのための情報システムの構築のように、専門的な部門にその実施を一定程度集中させたほうが良い場合や、社外持出しの許可のように、個別の部門ごとに実施させても良い場合もあり得るでしょう。

役割分担の一例については、「本章４－２　各部門の役割分担の例」を参照。

➢　情報収集体制の確立

日頃から、秘密情報の管理に係る情報が社内において適切に共有されるような体制を整えます。例えば、人事部門が退職予定者を把握した場合に、情報セキュリティ部門が、当該退職予定者のアクセスログのチェックを強化するなどの対応が可能となるような体制を検討します。

具体的には、各部門の担当者の情報共有の場を定期的に設けたり、情報共有のタイミングやその内容、情報共有ルート等について社内ルール化しておいたりすることが考えられるでしょう。

➢　情報漏えい事案対応に係るルール（マニュアル等）の策定

実際に情報漏えいが疑われる場合の対応について、誰が情報漏えいの兆候をチェックするのか、情報漏えいを検知した場合、どのような基準で、どのようなルートで、誰まで報告を行うのか、情報漏えいに対する初動対応や責任追及をどのように実施するのか等を、マニュアル等において事前に明文化します。また、実際に情報漏えいが生じた場合を想定して、そのマニュアル等に沿う形

で、部門間での情報共有、対策チームの招集、初動対応の手順、報道対応などを確認するための全社的な訓練（机上訓練・実地訓練）を行うことも重要です。このような訓練対応を通じて、そのマニュアル等自体の改善点が把握できることもあります。

その具体的に内容については、第６章を参照。

- 秘密情報の管理のチェック・見直し

秘密情報の管理に係る情報共有や内部監査、事後対応等を通じて自社の秘密情報の管理の実施状況を定期・不定期にチェックします。その結果、秘密情報の分類が不適切となっていたり、実施する対策が不十分となっていたりする場合には、必要に応じて、対策の実施を再徹底したり、その実施内容や、実施に当たっての社内体制・社内規程等について見直しを行います。

※内部監査等の実施に当たっては、毎回同一の観点からの監査を繰り返すだけでは効果が乏しくなるおそれもあるため、情報漏えいの手口の高度化・多様化の状況などを踏まえつつ、必要に応じて、内部監査等におけるチェックポイントなどを見直すことも重要。

- 周知徹底、教育、意識啓発

自社の秘密情報の定義や、秘密情報をどのように取り扱うべきかといったような秘密情報の管理に係る社内ルールについて、部門間で異なる理解や運用がなされないよう統一的な研修等を実施します。その際、必ずしも全従業員を対象とした周知、教育ばかりでなく、職務ごとの情報漏えいリスク・責務に応じた周知、教育を行うことも考えられます。なお、秘密情報の管理に係る社内表彰の実施や、情報漏えい者に対する懲戒処分の内容の周知（必要に応じて懲戒処分の内容に関する担当部門への事前の意見を行うこともあり得ます）なども、従業員等への意識啓発のために有効である場合があります。

部門横断的な組織と各部門の役割分担の事例

◆ **製造業・大規模の事例**
～全社的なモデルとその例外とのバランスがとれた仕組み～

部門・拠点が多いことから、中心的な部門において、秘密情報の管理についての原則的な方針を定めて、各拠点・各部門に示し、実際の運用の多くは各拠点・各部門の責任者を任命して行わせている。例えば、中心的な部門において、「極秘情報」、「秘情報」といった秘密情報の分類の方法や、「どのような情報を、どの分類として指定すべきか」といった考え方や事例についてのモデルを作成する。各拠点・各部門においては、そのモデルを基に、責任者が運用を行っているが、そのモデルとは異なったルールで情報管理を行いたいと考える場合には、各拠点・各部門から、その理由も合わせて中心的な部門へと伝え、それを許可するという仕組みとすることにより、全社的な統一と、各拠点・各部門の実情に沿った柔軟性のバランスを図っている。

（子会社・委託先等を含めた秘密情報の管理体制の構築）

○ 一定程度の事業規模を有する企業の場合、国内外を問わず、子会社や各地の支社を有しており、自社の秘密情報が共有する場合がありますが、当該子会社や支社においても、自社の秘密情報の管理に係るルールや対策が徹底されるようにすることが重要です。

○ また、委託先やサプライチェーンに関わる複数の企業など、他社に自社の秘密情報を共有する必要性がある場合、当該他社との関係で、秘密情報の対象やアクセス権者等の範囲を明確化し、共有化することや、当該他社における情報漏えい対策及びその実施体制の構築等を確保することが重要となります。

○ 具体的には、そのような観点から、当該他社との契約内容等を検討する必要があります。また、自社において統一的な対応がなされるよう、委託先等における秘密情報の管理体制の構築に係る当該他社との契約のあり方について、自社内でルール化しておくことも重要です。

パートナー企業やグループ企業を含めた管理体制の事例

◆ **電気機械器具製造業・大規模の事例**

～自社作成のチェックシートを共有し、取引先の情報管理水準を向上～

委託先企業や再委託先にも一定の情報管理水準が保たれるよう、委託契約の内容として、実施すべき情報管理策を具体的に盛り込んでいる。その一環として、自社が作成した情報セキュリティに係る基準やチェックシートを共有し、それらに基づく対策を講ずるよう求めている。同時に、委託先・再委託先も含めた情報セキュリティ研修を実施して徹底を図っている。

◆ **海外・電気機械器具製造業・大規模の事例**

～グループ全体で秘密情報保護ポリシーを共有～

外国拠点も含めたグループ全体で、統一化された秘密情報保護ポリシーを策定している。その際、各地域の法制度・ガイドライン・慣習などを検証し、最も情報漏えいリスクが高い地域を特定した上で、その地域を念頭に置いたポリシーを策定している。

４－２　各部門の役割分担の例

各部門がいかなる対策に責任を持つこととするかを分担することが、効率的かつ実効的であると考えられます。当然、このような役割分担でなければならないわけではありませんが、以下では、その役割分担の際の参考となるよう分担の一例を示します。

■　部門横断的な組織の事務局担当

（「保有する情報の把握・評価、秘密情報の決定」に関する役割）

- 「保有する情報の把握・評価、秘密情報の決定」の作業方針の決定などの全体取りまとめ

（情報漏えい対策に関する役割）

- 情報管理規程などの社内規程等の原案・見直し案の作成
- 秘密情報の管理に関する研修内容や実施方法の検討
- 部門横断的な組織（秘密情報管理委員会など）の事務運営

- 秘密情報の管理の実施状況の確認

（情報漏えい事案への対応に関する役割）

- 情報漏えい事案対応の際の全体調整（対策チーム等の招集・運営等）
- 「情報漏えい事案対応に係るルール・マニュアルの原案・見直し案の作成

■　法務担当

（情報漏えい対策に関する役割）

- 情報漏えいに関する訴訟対応の観点からの就業規則・情報管理規程等の確認
- 秘密保持契約・誓約書、委託契約等の各種契約の確認・ひな形の作成

※加えて、特に秘密保持義務契約書の管理（どのような情報について、いつまで、誰が、秘密保持義務を負っているのかといった情報の管理）も重要。

（「他社の秘密情報に係る紛争への備え」に関する役割）

- 転職者の受入れ、共同研究開発の場合等における法的リスク低減に関する相談
- 秘密保持契約・誓約書、共同研究開発契約等の各種契約の確認・ひな形の作成
- 他社からの警告書を受けた場合の対応の検討

（情報漏えい事案への対応に関する役割）

- 民事訴訟を提起する場合の訴訟対応の全体とりまとめ
- 刑事告訴をする場合の警察当局との窓口対応

■　人事・労務担当

（情報漏えい対策に関する役割）

- 法務担当との連携の下、就職時・退職時・異動時における適切な誓約書等の取得
- 部門横断的組織の事務局や法務担当との連携の下、情報漏えい防止の観点からの就業規則の見直し
- 教育・研修等の運営

※その内容や方法についても、部門横断的な組織の事務局のサポートを得なが

ら人事・労務担当が検討することとしてもよい

- 秘密情報漏えいに対する社内処分の実施・その内容の周知
- 働きやすい職場環境の整備に係る検討・実施や透明性が高く公平な人事評価制度の構築等
- 秘密情報の管理に係る意識共有、企業への帰属意識や働きがいを高める取組みの実施、防犯カメラの設置やログ取得、諸々の社内規程の整備に当たっての、労働組合との協議や取り決めの対応
- 退職者等の動向の把握

（「他社の秘密情報に係る紛争への備え」に関する役割）

- 法務担当との連携の下、適切な転職者の受入れの実施

（情報漏えい事案への対応に関する役割）

- 秘密情報漏えい者に対する懲戒等の実施

■情報システム担当（セキュリティ担当、ＩＴ担当）

（情報漏えい対策に関する役割）

- 社内規程等に沿ったＰＣ等へのアクセス権限の設定・変更等の実施
- 社内規程等に沿った情報システムの構築

  ※電子データの暗号化に係る設定、電子データ等の印刷・複製禁止に係る設定、私物ＵＳＢ等の使用禁止の設定、不許諾ソフトウェアのインストール禁止に係る設定、外部メールのチェックに係る設定、文書作成時の「マル秘」表示の自動的付加に係る設定、印刷者の氏名等の「透かし」の自動的付加に係る設定など
- 必要なログの取得・保管
- 不正アクセス等に対する防護システムの導入・運用

（「他社の秘密情報に係る紛争への備え」に関する役割）

- 他社情報を自社情報のサーバー等と別に保管する場合のサーバーの分離・仮想化（一台のサーバーを複数に分割して利用すること）に係る設定

（情報漏えい事案への対応に関する役割）

- 情報漏えいの兆候の把握や、その疑いの検知のためのログ確認等の実施
- 被害の拡大防止の観点からのネットワーク遮断の実施

- 証拠保全の観点から、ログ等の保全

■　経営企画・分析担当

（「保有する情報の把握・評価、秘密情報の決定」に関する役割）

- 経営戦略の観点からの情報の評価、秘密情報の決定時における助言

（情報漏えい対策に関する役割）

- 従業員等への周知を見据えた秘密情報の管理の企業の業務効率化等に対する貢献度の分析

（「他社の秘密情報に係る紛争への備え」に関する役割）

- 他社から受領する秘密情報を厳選する際の、経営戦略的観点からの助言

■　総務担当

（情報漏えい対策に関する役割）

- 部門横断的組織の事務局や法務担当との連携の下、情報漏えい防止の観点からの情報管理規程の見直し
- 来訪者受付・来訪者証の発行などの対応
- 工場見学等のマニュアルの作成・そのマニュアルに基づく対応
- 防犯カメラの設置
- コピー機やプリンター等における利用者記録・枚数管理機能の導入
- 施錠された部屋・保管庫等の鍵の管理
- 清掃業者、メンテナンス業者等との契約・各業者への対応

■　広報担当

（情報漏えい事案への対応に関する役割）

- 情報漏えいの事実の公表などに係るマスコミ対応の窓口

■　監査担当（内部統制担当）

（情報漏えい対策に関する役割）

- 秘密情報の管理の観点からの定期・不定期での内部監査の実施。その結果の部門横断的組織の事務局へのフィードバック（監査結果に基づく改

善指導、社内規程の改定に係る提言等）
- 情報漏えいに関する内部通報窓口の設置・運用

■　知的財産担当

（「保有する情報の把握・評価、秘密情報の決定」に関する役割）
- オープン＆クローズ戦略等の知的財産戦略の観点からの情報の評価、秘密情報の決定時における助言