資　料　５

企業における
秘密情報の保護・活用ハンドブック
～企業価値向上に向けて～
（案）

目　　次

第１章　目的及び全体構成

１－１　目的及び留意点等

（秘密情報の重要性）

○　企業が有する「情報資産」は、商品の生産、販売、サービスの提供などの様々な企業活動の価値や効率性を高めています。「情報資産」と一口に言っても、顧客情報、発明情報、ビジネスモデル、取引情報、人事・財務情報など多種多様であり、製品やサービスが均質化しつつある近年において、他者との差別化を図り、競争力を高めていくために、「情報資産」の保護・活用は、ますますその重要性を増しています。

○　そのような「情報資産」の中には、他者に対して秘密とすることでその価値を発揮する情報（秘密情報）が存在します。そのような秘密情報は、一度でも漏えいすれば、たちまち情報の資産としての価値が失われてしまい、その回復は非常に困難なものです。企業の経営に致命的な悪影響を与える場合もあるでしょう。

（本書の目的）

○　経営者は、秘密情報を含めた「情報資産」を企業活動の中でどのように有効に活用しつつ、その漏えいリスクにどのように対処していくかを、リーダーシップを持って判断していかなければなりません。そこで、本書では、秘密情報を決定する際の考え方や、その漏えい防止のために講ずるべき対策例、万が一情報が漏えいした場合の対応方法等を示しており、それによって、経営者を始めとする企業の方々に、自社における秘密情報の管理を適切に実施していく際の参考としていただくことを目的としています。

（本書と営業秘密管理指針との関係）

○　本書において漏えい対策の対象となる秘密情報は、不正競争防止法による保護の対象となる「営業秘密」と重なる場合もありますが、それだけではなく、企業において秘密として保持すべきと判断する全ての情報が対象となります。すなわち、本書で示す対策は、同法に基づく法的保護を受けるために必要となる水準[1]の対策とは

[1] 不正競争防止法に規定する「営業秘密」と認められるためには、その情報が、①秘密として管理されていること（秘密管理性）、②事業活動にとって有用であること（有用性）、③公然と知られていないことの３要件を満たす必要があります。①の秘密管理性が認められるためには、企業の「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によって、従業員に明確に示され、結果として、従業員がその意思を容易に認識できる（「認識可能性」が確保される）必要があります。

無関係のものであり、その水準を超えたグッドプラクティスや普及啓発的事項など、あくまで情報漏えいをできる限り防止することを目的とするものです。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については、営業秘密管理指針（平成２７年１月２８日改訂）[2]を参照ください。

（秘密情報管理の効用）

○　適切な秘密情報の管理を実施することにより、企業にとって致命的な悪影響を及ぼすおそれもある情報漏えいのリスクを減らすだけでなく、実効的な情報管理により、業務の効率性が高まり、業績の向上に繋がることを期待できます。また、退職者との関係で自社の秘密情報の対象範囲・内容を明確にすることは、転職に当たってのトラブルを防止し、働く方々の自由な職場選択・キャリアアップを可能とする環境の整備に繋がるとともに、企業にとっても、人材の流動性の向上を通じて多様な人材確保が可能となります。さらに、我が国企業の秘密情報の管理のレベルが底上げされることは、共同研究・開発における情報漏えいリスクを低減させ、オープンイノベーション[3]を更に進展させます。

○　このように、秘密情報の管理を実施することには、個別の企業や働く方々にとっても、社会全体にとっても、その実施に係るコストを上回る効用があると言えます。したがって、経営者の方々は、この点を踏まえ、一時的な秘密情報の管理に係る手間などを嫌うことなく、その実施に適切に取り組んでいただきたく思います。

（本書の留意点）

○　本書は、前述のとおり、企業の有する秘密情報の漏えいを防止するという観点からの様々な対策を示すものですが、情報管理に当たっては、本書で示すもの以外にも、情報を不正に改ざんさせないための対策（完全性の確保）や、システムダウンや災害時等にも情報が失われないようにするための対策（可用性の確保）なども重要となります。

○　また、秘密情報の漏えいの中には、従業員のミスによるものなど、漏えい者が意図しない形での漏えいも含まれますが、本書では、基本的に、意図的な秘密情報の漏えい防止を目的とした対策を紹介しています。ただし、本書において紹介する対策を実施することによって、意図的でない情報漏えいの防止にも相当程度の効果があるものと考えられます。

---

[2] http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/20150128hontai.pdf

[3] 企業の内部と外部のリソースを有機的に結合させ、新しい価値を創造すること（産学連携や企業間連携による共同研究など）

○　なお、本書では、本書策定の時点で有効であると考えられる対策を紹介しており、様々な技術の進展により、情報漏えいの手口やその対策が高度化・多様化するなどの状況の変化が生じた場合には、対策も、適時に見直されるべきものです。

１－２　本書の全体構成

（本書の全体構成）

○　第２章では、まずは自社が保有する情報の全体像を把握し、それを評価した上で、その中から秘密として保持すべき情報（秘密情報）を決定する際の考え方を説明します。

○　第３章では、秘密情報を同様の情報漏えい対策を講ずるものごとに分類する際の考え方と、具体的に講ずるべき対策等を示します。

○　第４章では、本書で示す様々な秘密情報の管理に係る方策をより実効的なものとするための社内体制のあり方を示します。

○　第５章では、他社の秘密情報に係る紛争に巻き込まれないため、又は万が一巻き込まれてしまったとしても正当にその立場を守るための対策を紹介します。

○　第６章では、自社の秘密情報が漏えいしてしまった場合の対応について説明します。

○　また、参考資料として、「各種契約書・規程等の参考例」や、「各種相談窓口等の連絡先」、「参考とすべき他のガイドライン等の一覧」、「営業秘密侵害罪に係る刑事訴訟手続における被害企業の対応の在り方について」、「競業避止義務契約の有効性について」を添付しています。

（情報漏えい対策の流れ）

○　上述のとおり、第２章から第４章にかけては、

- 自社が保有する情報を把握・評価した上で、秘密情報を決定・分類して、実施する情報漏えい対策を選択する。
- その内容について、社内においてルール化し、様々な状況の変化に応じて必要な見直しを行う

という情報漏えい対策の一連の流れとなっております。その流れを意識した上で第２章から第４章までを参照いただくと、より理解がしやすいものと考えられます。

１－３　本書の使い方

○　本書では、様々な秘密情報の管理に係る方策を、本章１－２のとおりの順番で示していますが、各企業においては、必ずしも本書に記載された全てを、記載された順番に沿って実施しなければならないものではありません。本書を読む時点で、どの程度の秘密情報の管理を既に実施しているかは企業によって大きく異なると考えられることから、例えば以下のように自社にとって特に参考となると考えられる箇所から読み始めていただいても構いません。

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っています。
・　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、業務効率の低下に繋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（第１章で示したステップ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、部署ごとに捜し出し、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はなく、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、ＰＣや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繋がります。

○　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[4]。

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[5]。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。

（把握にあたっての留意点）

○ 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ことではありません。「○△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把握すれば、後述の対策も立てやすくなります。

○ 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。

---

[4] 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。

[5] 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。

（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、上記（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[6]）、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か否か等、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。

【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

○ なお、ここで行う評価の最終的な目的は、自社の情報資産全体の評価ではなく、あくまでも「秘密情報の決定」であるため、把握した情報のうち、非公知情報のみを評価するということでも構いません。

※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

[6] 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。

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さ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)。

○　上記（１）（２）の作業により、自社が保有する情報にはどんなものがあるのか、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、そ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したり、標準化することを通じて他社にも自社技術を使用させる方が適切な情報もあれば、秘密として保持したり、権利化した上で独占実施したりするなど、自社のみで使用する方が適切な情報もあります。このように情報の性質を踏まえて情報を適切に活用しようとする考え方は、「オープン＆クローズ戦略」と呼ばれています。これに対し、顧客情報のような場合には、産業財産権化、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）等のコストと、保護により得られる利益（損害賠償額や侵害差止により得られる営業上の利益等）の比較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。

○　以下では、真に秘密として保持するべき情報を判断し、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　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出来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。

※なお、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、積極的には公開しないものの、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。

第３章　秘密情報の分類、情報漏えい対策の選択及びそのルール化

- 秘密情報の活用の促進、管理コストの適正化等の観点から、秘密情報の評価等に応じたメリハリのある情報漏えい対策を講ずることが重要です。そのためには、自社の秘密情報を、その評価の高低や情報の利用態様等に応じて、同様の対策を講ずるものごとに分類した上で、その分類ごとに適切な対策を選択することが必要です。
- 本章では、そのような「秘密情報の分類」に係る考え方や、講ずる対策を選択する際に参考となる具体例等を紹介します。（第１章で示したステップ２、ステップ３）
- 本章では、比較的簡易な管理方法から高度な管理方法まで様々な具体的対策例を提示していますが、その全てを実施しなければ情報漏えい対策として不十分ということではありません。本章で提示する対策を参考に、各社の企業規模、業種、秘密情報の性質、対策にかけることができる費用の多寡等の様々な状況に応じて、合理的かつ効果的と考えられる対策を適切に取捨選択･工夫して実施することが重要です。
- また、分類や対策は一度決めたら終わりではなく、情報のライフサイクル（生成→利用→保存→廃棄）におけるステージや様々な技術の進展等を考慮しつつ適宜見直していくことも重要です[7]。
- さらに、ここで記載する一連の流れを実効的にするためには、その内容を社内ルール化して社内で共有化しておくことも重要です。
- なお、第１章で述べたとおり、本章で示す対策を実施することは、秘密情報の漏えいを防ぐだけでなく、人材の流動性の向上を通じた多様な人材確保やオープンイノベーションの更なる進展にも寄与します。

３－１　秘密情報の分類

（分類の必要性）

○　第２章において、自社における「秘密として保持すべき情報」（秘密情報）が決定されることとなりますが、秘密情報は日々の業務の中で活用されてこそ価値を発揮するものであることを踏まえると、すべての秘密情報に一律に厳格な管理を行うことは、円滑な業務の実施に支障を及ぼし、また管理コストの無用な増大を招く結果となります。例えば、企業活動に不可欠な情報であっても、漏えいをおそれるあまり、金庫のように常時鍵を掛けて誰も開けてはならない場所に保管して事業活動に一切使わないのでは情報が活用されず、資産としては無価値なものとなります。情報の活用と保護のバランスを考慮した管理方法を検討していくことが重要です。

---

[7] 特定非営利活動法人日本ネットワークセキュリティ協会「中小企業情報セキュリティ対策促進事業」ＨＰ（http://www.jnsa.org/ikusei/01/02-02.html）参照

○　そのためには、各企業で取り扱う秘密情報の性質やその評価の高低、その利用態様等の事情に応じ、秘密情報を同様の対策を講ずるものごとに分類した上で、その分類ごとに必要な対策をメリハリをつけて選択することが重要です。

（分類に当たっての考え方）

○　秘密情報の分類においては、まず、第２章２－１において行った情報の評価の結果を考慮し、評価の高い情報ほど厳格な対策を行うことが考えられます。

○　一方で、同程度の評価の秘密情報であっても、以下のような「情報の利用態様」に応じて、異なる対策を講ずる場合もあります。

※「情報の利用態様」は予め定められたものではなく、自社の事業規模や業種、取り扱う情報の性質等を踏まえた上で、望ましい「情報の利用態様」とは何かを自主的に判断することが重要です。

例えば､その秘密情報は､｢従業員各々に個別に資料を所持させるべきものなのか、共有資料のみとするのか」や､「インターネットワークに接続されたＰＣ等に保管すべき情報か否か」といったことを今一度検討してみることが有効です。

【情報の利用態様として考慮すべき観点の例】

- **個々の従業員が手軽に閲覧・持出し・利用等をできるようにしておかなければ日々の業務遂行が困難となる情報か否か（例：従業員が営業を行うに当たって頻繁に用いる顧客情報）**
- **情報に対するアクセス権者の範囲が広くならざるを得ない性質のものか否か（例：世界各地の研究拠点と共有する実験データ）**
- **その情報を活用する従業員の職務は何か**
- **外部ネットワークに接続されＰＣ等に保管されることが多い情報か否か**
- **顧客や取引先に開示することが多い情報か否か**
- **日々更新される情報か否か（開発情報、顧客情報など）**

※「同程度の評価の情報でも異なる対策を講ずる場合」とは、例えば、個々の従業員が手軽に閲覧・持出し・利用等をできるようにしておくべき情報については、他の情報に比べ簡易な管理を行うことが望ましいといったような場合や、情報に対するアクセス権者の範囲が広くならざるを得ない情報については、５つの「対策の目的」（後述）のうち、「接近の制御」に係る対策よりも、「視認性の確保」に係る対策を重点的に選択することが有効であるといったような場合を指します。

○　また、個人情報保護法に基づく管理が求められる個人情報や、他社から秘密保持義

務を負った状態で受領した情報など、「法令や他社との契約に基づく特別の管理」を求められる情報については別の対策を講ずる分類とすべき場合もあります。

○　このように、情報の評価の高低の観点に加えて、「情報の利用態様」や「法令や他社との契約による特別の管理」の観点から、別の対策を講ずる分類を設けることも考えられます。

※社内の統一的なルールでは、情報の評価の観点からの分類のみ設けておき、例えば各部門の管理責任者が行う「分類の指定」等の運用の段階において、「情報の利用態様」や「法令や他社との契約に基づく特別の管理」の観点を考慮するといったことも考えられます。

○　なお、分類の数については、各企業において適正と考えられる分類数は異なるものと考えられますが、あまりに多くの分類数としてしまうと、情報管理が煩雑となり対策が徹底されなくなってしまうなど、対策の有効性・効率性を低減してしまうおそれがあることに留意します。

３－２　分類に応じた情報漏えい対策の選択

（対策の選択に当たっての考え方）

○　本章３－１において設定した秘密情報の分類ごとに、具体的にどのような情報漏えい対策を講ずるのかを選択します。その際には、誰に対して対策を行うのか（従業員、退職者、取引先、外部者）、どのような形で秘密情報が存在しているのか（情報にネットワークを介してアクセスすることができるか、工場ライン等の物件自体が秘密情報である場合か否か等）、漏えいの手口やその動機がいかなるものであるかといった状況によって効果的な対策は異なることに留意する必要があります。加えて、転職者の増加や、様々な契約形態に基づく人事やグローバル人材の登用など、各社の事情に応じた対策を選択することが有効です。

（５つの「対策の目的」）

○　情報漏えい対策は、目的を考えずに闇雲に実施してしまうと、業務への過度な制限や、無駄なコストが発生しかねません。したがって、情報漏えいに対し、それぞれの対策がどのような効果を発揮するのかといった目的を意識し、効果的・効率的な対策を選択することが望まれます。

○　そこで、本章においては、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、以下の５つの「対策の目的」を設定した上で、それぞれに係る対策を提示して

います。

【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。

（２）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。

（３）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つく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。

（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）

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。

※なお、ここで紹介する対策のうち、「秘密情報の取扱い方法等に関するルールの周知」、「秘密保持契約等（誓約書を含む）の締結」、「秘密情報であることの表示」といった対策は、不正競争防止法上の「営業秘密」の要件である、「秘密管理性」を満たすために必要な「認識可能性（第１章１－１参照）」の確保につながるものであると考えられます。

（５）企業への帰属意識・信頼関係の向上等

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。これらの取組によって、職場のモラルを維持することを目的とします。

一方、取引先との関係においては、信頼関係を向上させることを目的としています。

○ なお、本書で示す対策のうち、「接近の制御」、「持出し困難化」、「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）」に資する対策の中には、従業員のミスによる漏えいの防止にもつながります（アクセス権限の階層的制御、情報の暗号化、遠隔操作によるデータ消去機能を有するＰＣの利用、秘密情報であることの表示など）。

（対策の選択の方法）

○ 本章冒頭で述べたとおり、本章では、比較的簡易な管理方法や、より高度な管理方法など、様々な難易の対策を提示していますが、そのすべての対策を実施しなければ、情報漏えい対策として不十分ということではありません。本章で提示する対策を参考に、各社の企業規模や業種、秘密情報の評価や利用態様、対策にかけることができる費用の多寡等の様々な状況に応じて、合理的かつ効果的と考えられる対策を適切に取捨選択・工夫して実施することが重要です。

○　また、５つの「対策の目的」を考慮しながら、バランス良くそれぞれの目的に応じた対策を選択していくことが重要です。企業の規模、保有する情報の性質、その情報をどのような利用態様で活用するのかといった事情を考慮して、重視すべき「対策の目的」を選択して、ムリ、ムダ、ムラの無い形で対策を講じていくことが考えられます。

３－３　秘密情報の取扱い方法等に関するルール化

（１）ルール化の必要性とその方法

○　本章に記載するステップを通じて、決定された対策を実効的に講じていくためには、その内容を社内でルール化することが必要です。

○　ルール化の方法としては、就業規則、情報管理規程といった社内の規程を策定することが一般的です。いずれの場合においても、従業員等が、秘密情報の管理を適切に行うことができるよう、秘密として保持すべき情報、その取扱い方法について理解できる内容としておくことが重要です。

※ルール策定に当たっては、従業員とのコミュニケーションを十分に取りながら進めることが、透明性確保・従業員の認識の向上を図るために重要です。

（２）秘密情報の取扱い等に関する社内の規程の策定

○　秘密情報の管理について社内の規程を策定することは、秘密情報の取扱い等に関するルールを社内に広く周知するための手段として効果的です。

○　従業員等が秘密情報の取扱いや、秘密情報に関して秘密保持義務が課されていること等について、十分理解できるようにするため、社内の規程には以下の内容を盛り込んでおきます。

（社内の規程に盛り込んでおくとよい条項）

※条項によっては、その詳細が規程に基づいて別途作成される細則や別紙等に記載される場合もあります。

①適用範囲

：役員、従業員、派遣労働者、委託先従業員（自社内において勤務する場合）等、本規程を守らなければならない者を明確にします。

②秘密情報の定義
③秘密情報の分類
：分類の名称（例えば「役員外秘」、「部外秘」、「社外秘」など）及び各分類の対象となる秘密情報について説明します。
④秘密情報の分類ごとの対策
：「秘密情報が記録された媒体に分類ごとの表示をする」、「アクセス権者の範囲の設定」、「秘密情報が記録された書類を保管する書棚を施錠管理して持出を禁止する」、「私物のＵＳＢメモリの持込みを制限し複製を禁止する」、など、分類ごとに講じられる対策を記載します。
⑤管理責任者
：秘密情報の管理を統括する者を規定します。
⑥秘密情報及びアクセス権の指定に関する責任者
：分類ごとの秘密情報の指定やその秘密情報についてのアクセス権の付与を実施する責任者について規定します。
⑦秘密保持義務
：秘密情報をアクセス権者以外の者に開示してはならない旨などを規定します。
⑧罰則
：従業員等が秘密情報を漏えいした場合の罰則を定めておきます。

○　なお、社内の規程を周知して、従業員等に秘密情報の取扱い等について理解を深めることは、それ自体が「秘密情報に対する認識向上」に資する対策となります。

３－４　具体的な情報漏えい対策例

○　ここでは、従業員等、退職者等、取引先、外部者それぞれごとに、５つの「対策の目的」に応じて有効と考えられる対策例を提示します。

（１）従業員等に向けた対策

（従業員等とは）

従業員等とは、典型的には役員や自社が雇用する従業員が該当しますが、自社内の実習生や派遣労働者、委託先従業員であって自社内において勤務する者なども含みます。

（留意点）

なお、自社が直接雇用する者以外に対しては、「企業への帰属意識の向上等」の観点からの対策は効果が乏しい場合もあるため、それ以外の「対策の目的」の観点からの対策を着実に実施していくことが重要です。

①「接近の制御」に資する対策

ここで紹介する対策は、

ａ．ルールに基づく適切なアクセス権の付与・管理

を実施して、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、

ｂ．情報システムにおけるアクセス権者のＩＤ登録

ｃ．分離保管による秘密情報へのアクセスの制限

ｄ．ペーパーレス化

ｅ．秘密情報の復元が困難な廃棄・消去方法の選択

といった、対策を講ずることで、秘密情報に対するアクセス権（秘密情報を閲覧・利用等することができる権限）を有しない者を秘密情報に近づけないようにすることを目的としています。

ａ．ルールに基づく適切なアクセス権の付与・管理

○ 社内規程等において、秘密情報の分類ごとに、アクセス権の設定に関するルール（どのような手続きで誰が設定するのかなど）を明確にした上で、当該ルールに基づき、適切にアクセス権の範囲を設定します。

○ アクセス権の範囲については、その秘密情報の内容・性質等を踏まえて、「知るべき者だけが知っている（ need to know ）」という状態が実現するようにすることが重要です。その秘密情報を知る必要がない者にまでアクセス権を付与してしまうと、情報漏えいリスクを不必要に高めてしまうこととなります。

○ 人事部門との情報共有を円滑にすること等により、異動等に伴うアクセス権の変更を迅速に実施して、常に、アクセス権者の範囲が適正に設定されているようにすることも考えられます。

○ 例えば、人事異動、プロジェクト終了時などについては、アクセス権の範囲を適切に変更することが重要です。また、出向等によって他組織に就業する者についても一時的にアクセス権を停止する等の対応を行うことが考えられます。

（漏えいリスクを低減するためのアクセス権設定の具体例）

- 工場の作業ライン等について、作業の一連の流れを複数人で分担するなど、工程全体の情報を１人の作業員が把握できないようにアクセス権の範囲を設定する。実習生に開示する情報の範囲についても注意する。
- 従業員等の個人ではなく、業務や役職に基づきアクセス権を設定することで、人事異動等に伴って適切にアクセス権が設定・変更されるように

する。

※特に情報システムにおいては、「ロールベースアクセス制御」[8]に対応したアクセス制御システムを導入して、アクセス権の範囲を業務にひも付して、人事異動に対応して適切にアクセス権が設定・変更されるように設定することも有効です。

ｂ．情報システムにおけるアクセス権者のＩＤ登録

○ 予め、従業員等に対して情報システム上のＩＤを付与し、そのＩＤを認証する（ＩＤを使用する者が本人であることを確認する）ためのパスワード[9]等を設定しておきます。

※ＩＤ・パスワードは複数の従業員間で同じものを使い回さないことが重要です。

※パスワードの設定に当たっては見当をつけられやすいパスワードは避けることが重要です。また、パスワードに有効期限を設定し、長期間にわたり同一のパスワードを使用しないことも有効です。

○ ａ．により決定されたアクセス権者だけが、利用することが許可された電子データ等（ｃ．に記載の電子データ、分離されたフォルダやサーバー等）にアクセスできるように、ＩＤを登録します。

※電子データやフォルダへアクセスするためのＩＤをＰＣに登録した上で、登録されたＩＤに限定して電子データや分離されたフォルダにアクセスすることができるよう、最もよく使われているＯＳの機能を活用して設定することができます。

※情報システム上のＩＤ登録作業は、複数人のシステム管理者で行うことで、適正な実施を確保することができます。

ｃ．分離保管による秘密情報へのアクセスの制限

○ 秘密情報が記録された書類・ファイルや記録媒体（ＵＳＢメモリ等）については、保管する書棚や区域（倉庫、部屋など）を分離し、電子データについては格納するサーバーやフォルダを分離した上で、アクセス権を有しない者が、その秘密情報を保管する領域にアクセスできないようにします（秘密情報が保管された部屋に入室できない、保管庫を開扉できない、サーバーにアクセスできない状態とする等）。

---

[8] 情報システムにおいて個人ではなく職務（役割）に対してアクセス権限を割り当てること（IPA（独立行政法人情報処理推進機構）「組織における内部不正防止ガイドライン」ｐ．２９を参照）。

[9] IPA がＷｅｂにパスワードの安全性を高めるための管理方法について分かり易くまとめたページ（「チョコっと＋パスワード」）掲載していますのでご参照ください。（http://www.ipa.go.jp/chocotto/pw.html）

○ なお、全ての秘密情報について、厳格なアクセス制限を講ずることが難しい場合も考えられますので、秘密情報の評価の高低や利用態様に応じて、対策を選択していくことが重要です。

（具体的な管理方法）

- **書類・ファイル、記録媒体を書棚や区域（倉庫、部屋など）に保管し施錠管理。**
  - ex）**業務時間のみ解錠する。（同時に、業務時間中についてはアクセス権を有しない者が入室・閲覧しないように視線を配るなど、視認性を高めておくことが重要。）**
  - ex）**管理者が鍵を管理し、入退室の際の鍵の貸し出しは許可制にする。**
  - ex）**重要度の高い情報等については、認証システム導入による入退室管理を実施する。**
    - ※認証システムとしては、ＩＣカード認証、生体認証（指紋認証、こう彩認証、静脈認証等）、ワンタイムパスワード（時刻同期方式、イベント同期方式、チャレンジレスポンス方式等）、ＰＩＮ入力の付与等があり、アンチパスバック機能[10]も併用できる。なお、これらのシステムのうち、製品によっては、入退出者や入退出時刻等を記録する機能を持つものもあるが、その記録を保存することは「視認性の確保」にもつながる。
  - ex）**重要度の高い情報等については、警備システムの導入、警備員の配置**
- **電子データの管理**

  以下のような方策で秘密情報が記録された情報の分離等を行った上で、アクセス権を有する者のＩＤからのみアクセスできるようにする。
  - ※フォルダや電子データについて、アクセスに必要なパスワードを設定して管理する方法も考えられるが、個別ＩＤ付与を行わないままに共通パスワードのみで管理する場合、万一の場合に追跡が困難になるケースがあることに注意。また、人事異動や退職等によってアクセス権を失った者が、その後も、そのフォルダや電子データにアクセスできることがないよう、その都度パスワードを変更することが重要。
  - ex）**秘密情報をネットワークに接続しない特定のＰＣに保存**
    - ※当該ＰＣを施錠管理する区域に保管し、アクセス権者のみが作業できるようにすることも考えられる（区域における施錠管理）。

[10] 入室していない ID では退室できず、退室していない ID では入室できない等、同じ ID で続けて入退室できないようにする機能。

ex）アクセス権を有する者のＩＤでログインしたＰＣ等からのみその電子データを閲覧できる状態にする。

ex）フォルダの分離

ex）サーバーの物理的分離（複数台のサーバーに分離）、
サーバーの仮想化による論理的分離（1 台のサーバーを複数の仮想サーバーに分割）

ex）ネットワークの分離（複数のＬＡＮを構築）

※上記方策は、組み合わせて利用することも考えられる。

※重要度の高い情報の場合は、ＰＣ、サーバー等へのアクセスに当たって、ＩＣカードによる認証システム（前述）を導入することも考えられる。

- 生産ラインのレイアウト等

ex）生産ラインのレイアウト等、その「物」自体が秘密情報であるものが置かれた工場等を施錠管理。

ｄ．ペーパーレス化

○ 自社内の秘密情報をペーパーレスにして、アクセス権を有しない者が秘密情報に接する機会を少なくします。加えて、電子化された秘密情報について、印刷やコピーができない措置を施せば、更に持出し困難化に資することになります。

○ 例えば、ペーパーレス化し、情報を社内共通のデータベースといった形で活用することは、日々更新される情報の最新の状態について、従業員間での共有化が促進されることになります。更に、従業員が相互にアイディアを出し合うなどの活動が利便となることにより、共有知識の更なる高付加価値化や作業の効率化にも役立ちます。

○ なお、完全なペーパーレス化を実施することが難しい場合でも、電子化された秘密情報について、印刷できるデータの内容や、印刷できる者、印刷の目的等を限定するというルールを設け、併せてその印刷物の廃棄方法にも留意することで、同様の効果が得られます（廃棄方法についてはｅ．に記載）。

ｅ．秘密情報の復元が困難な廃棄・消去方法の選択

○ 秘密情報が記録された書類・ファイルや記録媒体等の廃棄、秘密情報が記録された電子データの消去を行う場合、アクセス権を有しない従業員等が、廃棄・消去された情報を復元して、その情報にアクセスすることができないように、以下のように復元不可能な形にして廃棄・消去します。

（具体的な廃棄・消去方法）

- **書類の廃棄方法**
  - ex）シュレッダーにより裁断し、廃棄。
    - ※秘密情報の重要度に応じて、より復元を困難とするため、クロスカット（縦方向と横方向の両方から裁断する）方式のシュレッダーを利用するなど、かけることができる費用の多寡も踏まえながら、シュレッダーの機能性について検討することも重要。
  - ex）秘密情報を廃棄するゴミ箱は、廃棄後取り出すことができない鍵付きゴミ箱に限定。
  - ex）重要度の高い情報等については、信頼できる専門処理業者に依頼して焼却・溶解処分。場合によっては、その証明書を発行してもらう。
- **秘密情報を保存していた記録媒体（ＵＳＢメモリ等）、ＰＣ、サーバーの廃棄方法**
  - ex）市販されている完全消去するソフトや、磁気記録方式のハードディスク磁気破壊サービス等を利用してデータを消去の上、その記録媒体等を物理的に破壊（記録媒体からデータを消去しただけでは復元されるおそれがあるため）。

②「持出し困難化」に資する対策

ここで紹介する対策は、秘密情報が記載された会議資料等の回収、従業員の私物ＵＳＢ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、持ち出したりすることを物理的、技術的に阻止することを目的としています。具体的には、どのような形で情報が持ち出されるのかといった持ち出しの態様（【書類、記録媒体、物自体等の持出しを困難にする措置】、【電子データの外部送信による持出しを困難にする措置】、【秘密情報の複製を困難にする措置】、【アクセス権変更に伴いアクセス権を有しなくなった者に対する措置】）に応じて、対策を整理して記載しています。

【書類、記録媒体、物自体等の持出しを困難にする措置】

ａ．秘密情報が記された会議資料等の適切な回収

○　アクセス権を有する従業員等であっても、個別には資料を所持させないこととした上で、会議等で資料を配布した場合には、終了後、回収します（資料に、通し番号を付すことで遺漏なく回収することが可能です。）。従業員等の手元に資料を残させないことにより、資料を持ち出すことができない状態にします。

ｂ．秘密情報の社外持出しを物理的に阻止する措置

○　ノートＰＣ等を持ち出せないようセキュリティワイヤーで固定します。

○　退社時の荷物検査や、セキュリティタグによる退社時の情報持出しのチェック等の対策を講じることも考えられます。

※例えば、秘密情報が記載・記録された紙や記録媒体、それ自体が秘密情報である物件に検知タグを取付けた上で、出入り口に検知ゲートを設置し、不正な持出しの場合に警報が鳴るようなシステムを導入することが考えられます。

ｃ．電子データの暗号化による閲覧制限等

○　電子データを暗号化しておくことで、アクセス権がない従業員等が当該データを入手することができたとしても、閲覧ができないようにします[11]。

○　電子データのアクセス権を有するＩＤでログインしたＰＣ等からのみ当該電子データを閲覧できるようにします。

---

11 IPA「暗号化による＜情報漏えい＞対策のしおり（https://www.ipa.go.jp/security/keihatsu/announce20140320_2.html）」に暗号化の概要、注意事項が記載されています。

ｄ．遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用

○　ＰＣ等が盗難された場合などに備えて、以下の市販のツールを利用することが考えられます。

（消去機能の例）

- 遠隔操作によりＰＣ内のデータを消去できるツール。
- 情報機器について、パスワードロックで、一定の回数認証に失敗すると重要情報を消去するツール。
- 一定期間、管理サーバーとのやり取りがなされない状態が続いた場合に指定したデータが自動的に消去されるサービス。
- 電子データそのものに遠隔操作による消去機能を備えさせるツール。

【電子データの外部送信による持出しを困難にする措置】

ｅ．社外へのメール送信・Ｗｅｂアクセスの制限

○　電子データについて、メールに添付できない設定としたり、メールの送信容量を制限したりすることで、秘密情報である電子データを、メール送信によって外部に持ち出すことを防止・困難化します。

○　コンテンツフィルタを導入して、ＳＮＳ、アップローダー及び掲示板等へのアクセスを制限し、Ｗｅｂアクセスによる持出しを防止・困難化します。

ｆ．電子データの暗号化による閲覧制限等（再掲）

○　電子データを暗号化したり、登録されたＩＤでログインしたＰＣからしか閲覧できないような設定にしておくことで、外部に秘密情報が記録された電子データを、無断で、メールに添付して送信しても、閲覧ができないようにします。

ｇ.遠隔操作によるデータ消去機能を有するＰＣ･電子データの利用(再掲)

○　電子データそのものに遠隔操作による消去機能を備えておくことで、無断で外部にデータが送信された場合に消去することができます。

【秘密情報の複製を困難にする措置】

ｈ．コピー防止用紙やコピーガード付の記録媒体・電子データ等により秘密情報を保管

○　秘密情報が記載された書類について、市販のコピー偽造防止用紙（コピーでき

ないものや浮き出し文字によって不正コピーであることを明らかにするもの等）を使用することで、不完全な複製物しか作成できないようにします。

○ 電子化された秘密情報について、印刷、コピー＆ペースト、ドラッグ＆ドロップ、ＵＳＢメモリへの書き込みができない設定としたり、コピーガード付きのＵＳＢメモリやＣＤ－Ｒに保存することで、秘密情報の複製を制限します。

ｉ．コピー機の使用制限

○ 従業員等のＩＤカードとコピー機を連動させ、同一のＩＤカードで１日当たりに印刷できる枚数を制限することにより、一度に資料全体の複製物を作成することを困難にします。

ｊ．私物のＵＳＢメモリや情報機器、カメラ等の記録媒体・撮影機器の業務利用・持込みの制限

○ 社内におけるＰＣやＵＳＢメモリ等の記録媒体の利用は会社貸与品のみとした上で、私物の記録媒体の持ち込みを制限して、秘密情報の私物記録媒体への複製ができないようにします。この対策を徹底するために、ＵＳＢの差込口のないものやＵＳＢの差込口を無効化したり、物理的にふさぐ部品を取り付けたＰＣを利用することが考えられます。

○ 合わせて、私物のＵＳＢメモリ等の持込みや業務での利用がなされていないかを確認することも重要です。

※私物の記録媒体等の業務利用を認める場合には、利用できる業務範囲や利用に当たって遵守すべき事項等のルールを定めることが重要です[12、13]。

○ 私物のスマートフォンについて、重要な秘密情報が保管されている書庫や区域など、特に情報漏えい対策を厳格に行うべき区域に限って、持込みを制限することが考えられます。

○ 生産ラインのレイアウトなどについては、その工場へのカメラ等の撮影機器の持込みを制限し、写真撮影を通じた情報の持出しを困難にします。

---

[12] IPA「組織における内部不正防止ガイドライン」p.36 を参照

[13] 私物端末の業務利用の際のリスクやセキュリティ対策等については、「私物端末の業務利用におけるセキュリティ要件の考え方（平成 25 年 3 月　各府省情報化統括責任者（ＣＩＯ）補佐官等連絡会議ワーキンググループ報告)」が参考になる。
（https://www.kantei.go.jp/jp/singi/it2/cio/hosakan/wg_report/byod.pdf)。

【アクセス権変更に伴いアクセス権を有しなくなった者に対する措置】

ｋ．秘密情報の消去・返還

○ プロジェクトに参加する従業員等に秘密情報を示す際に、秘密保持契約等において、プロジェクト終了時の秘密情報の消去・返還について定めておきます。これに基づき、プロジェクト終了時には、当該従業員等が有している秘密情報が記録された書類や記録媒体等を返還させ、秘密情報である電子データを消去させます。

※記録媒体等の返却時には、その記録媒体や内部に記録されたデータに対して、利用者が設定したパスワードも提出させるようにします。

○ この措置の実効性を確保するためには、上記の「h. コピー防止用紙やコピーガード付の記録媒体・電子データ等により秘密情報を保管」で紹介したような、複製のできない形で秘密情報を共有しておくことが必要となります。

③「視認性の確保」に資する対策

ここで紹介する対策は、職場のレイアウト変更、防犯カメラの設置といった【目につきやすい状況を作りだす対策】、情報システムにおけるログの記録・保存といった【事後的に検知されやすい状況を作り出す対策】により、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させ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。

更に、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るたりすることなど、【管理の行き届いた職場環境を整える対策】により、情報管理に関心の高い職場であると認識させ、心理的に漏えいしにくい状況をつく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。

【管理の行き届いた職場環境を整える対策】

ａ．職場の整理整頓（不要な書類等の廃棄、書棚の整理等）

○ 不要となった書類が廃棄されておらず、様々な資料が乱雑に積まれ、整理がなされていない状態となっていると、職場全体が情報管理に対して無関心であるとか、無責任であることを情報漏えい者に連想させ、情報漏えいを行ったとしても発覚しないと思わせることになってしまいます。

○ 書類等の必要性を適切に判断した上で不要なものは廃棄するとともに、書棚の整理や、職場の清掃等を実施することで、情報漏えいを行おうとする者に対して、情報管理に係る関心が高く、管理が行き届いた職場であると認識させることにつながります。

○ 加えて、自社情報が整理されることにより、情報検索が容易になり、業務効率が向上することも期待できます。

ｂ．秘密情報の管理に関する責任の分担

○ 従業員等のそれぞれが、秘密情報の管理についての責任を分担する（責任者が不明の状態を作らない）ことで、情報管理に対する当事者意識を高めます。

ｃ．「写真撮影禁止」、「関係者以外立入り禁止」の表示

○ 秘密情報が保管されている書庫や区域（倉庫、部屋など）の出入口に「写真撮

影禁止」、「関係者以外立入り禁止」といった掲示を行うことにより、情報管理に係る関心が高く、管理が行き届いた職場であると認識させるようにします。

【目につきやすい状況を作り出す対策】

ｄ．職場の座席配置・レイアウトの設定、業務体制の構築

○ 従業員同士で互いの業務態度が目に入ったり、背後から上司等の目につきやすくするような座席配置としたり、秘密情報が記録された資料が保管された書棚等が従業員等からの死角とならないようにレイアウトを工夫します。

※なお、取り扱う情報によっては、アクセス権のない従業員等から画面を容易に見られることによって秘密情報が漏えいしてしまうことを防ぐために、座席配置・レイアウトを検討すべき場合もあります 。

○ また、秘密情報を取り扱う作業については、可能な限り複数人で作業を行う体制を整えます。単独作業を実施する場合には、各部門の責任者等が事前に単独作業の必要性、事後には作業内容を確認するようにします。

ｅ．従業員等の名札着用の徹底

○ 従業員等に社員証や名札の着用を徹底させ、他者から自己の氏名や所属部署が確認でき、情報漏えい行為を目撃された場合に、すぐさま自己の氏名等が特定されてしまう状況とすることにより、「見えやすさ」を確保します。

ｆ．防犯カメラの設置等

○ 秘密情報が記録された書類・電子媒体が保管された書庫や区域など、秘密情報の不正な取得や複製の現場となり得る場所に防犯カメラを設置して、情報漏えい行為を行おうとする者に「見られている」という認識を持たせるようにします。合わせて、当該場所から会社の外へと向かう動線に対しても防犯カメラが向けられていると、より効果的です。

○ この対策は、秘密情報の保管区域にアクセス権者のＩＣカードでのみ入室を可能としている場合に、アクセス権を持たない者がアクセス権者のＩＣカードを使用して入室したり、アクセス権を持たない者がアクセス権者と一緒に入退室することを防止するなど、アクセス権者とＩＣカードの使用者の同一性を担保し、①「接近の制御」を補完する効果もあります。

○ 視認性の効果を高めるためには、見えやすいところに防犯カメラを設置するとともに、そのそばに「防犯カメラ作動中」といった掲示をすることが考えられ

ます。

※この掲示は、本対策の効果を高めるとともに、従業員等が知らない間に撮影されていたということがないようにする意味でも重要です。

○ 抑止力の観点からは、必ずしも全時間帯の映像を記録しておく必要はないものの、情報漏えい行為者に対する責任追及の際に必要となる証拠の確保の観点からは、より多くの時間帯で映像が記録されていることが望ましいと考えられます。

ｇ．秘密情報が記録された廃棄予定の書類等を従業員の目の届くところに保管

○ 秘密情報が記録された廃棄予定の書類等を、実際に廃棄するまでの間、複数の従業員等の目の届く場所に保管します。

ｈ．外部へ送信するメールのチェック

○ 外部へのメール送信の際に、その全てのメール又は一部のメールについて、自動的に上司等にもＣＣメールが送信されるよう設定したり、従業員のメールの送受信内容を必要に応じて閲読する場合があることを周知したりするなど、外部とのメールでのやり取りが上司等に把握される可能性があると認識させることで、メールでの情報漏えい行為を行いにくい状況をつくります。

※本対策を講じる前提として、「社内メールの業務目的以外の使用を禁止していること」、「メールのやりとりをモニタリングする可能性があること」を予め就業規則等の規程に盛り込んでおく等して社内に周知し、従業員等のメールが知らない間にチェックされていたということがないようにすることが重要です[14]。

※直接、「視認性の確保」につながるわけではないものの、そもそも一定以上の役職の従業員でなければ外部へとメールを送信できないよう設定するということも考えられます（「持出し困難化」につながる対策）。

ｉ．内部通報窓口の設置

○ 従業員等が、他の従業員等の情報漏えい行為と思わしき行為を確認した場合の通報窓口を設置し、窓口が設置された旨を周知します。

○ また、内部通報を無用に躊躇することがないよう、匿名での私書箱等を設置す

[14] 従業者のモニタリングを実施する上での留意点については、「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」p.40 が参考になる。
（http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212guideline.pdf）

るなど通報者の匿名性を確保する工夫を行います。この場合、内部通報者に不利益を及ぼさないように配慮することも重要です。

○ なお、自己の属する部門以外の部門へと通報することが可能となるよう、複数部門において窓口を設置することが考えられます。

【事後的に検知されやすい状況を作り出す対策】

ｊ．秘密情報が記録された媒体の管理等

○ 秘密情報が記録された書類、ファイル、記録媒体（ＵＳＢメモリ等）を、共有して書庫等に保管するとともに、それらの複製を禁止した上で、保管する媒体等に通し番号を付けて管理します。これによって資料の不足や欠損が生じた場合にすぐに把握できるようにします。

○ さらに、共有保管された書類、ファイル、記録媒体を貸し出す場合には、誰にどの記録媒体を貸し出しているかわかるように、貸出し時及び返却時に、その日時、氏名、貸し出した資料名等を記録して管理します。資料の重要性によっては、貸出しを許可制とすることも考えられます。

ｋ．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

○ 従業員等のＩＤカードとコピー機やプリンター等とを連動させることによって、ＩＤカードによる認証がなければ印刷ができないように設定した上で、コピー機やプリンター等を、誰が、いつ利用したか、どのような資料を何枚印刷したか等を記録します。

ｌ．印刷者の氏名等の「透かし」が印字される設定の導入

○ 秘密情報が記載された電子データを印刷した場合に、強制的に印刷者の氏名やＩＤの「透かし」が印字されるように設定することにより、印刷物の外観から、誰が印刷したものかがすぐ分かるようにします。

ｍ．秘密情報の保管区域等への入退室の記録・保存とその周知

○ 秘密情報が記録された媒体等を分離保管している区域への入退室について記録を取る（台帳管理、ＩＣカードや生体認証等）とともに、その旨を周知します。

※職場の出社・退社時間の記録をとることも考えられます。

ｎ．不自然なデータアクセス状況の通知

○　深夜帯や休日に、複数分野の業務にわたる様々なデータにアクセスし、大量のダウンロードがなされているなど、不自然な時間帯・アクセス数・ダウンロード量を検知した場合に上司等に通知がなされるようにした上で、その旨を社内に周知します。

ｏ．ＰＣやネットワーク等の情報システムにおけるログの記録・保存とその周知

○　ＰＣやネットワーク等において、誰が（利用者ＩＤの記録）、どの端末から、いつ、どの秘密情報にアクセスされたか（アクセス履歴）、どのような操作をしたか（Ｗｅｂページへのアクセス履歴や、メールの送受信履歴等）といったログを取得し、保存します。加えて、ログを記録・保存していることについては事前に社内に周知しておきます。

※「社内ＰＣの業務目的以外の使用を禁止していること」、「アクセスログをモニタリングする可能性があること」を、予め就業規則等の規程に盛り込んでおく等して社内に周知することが考えられます。この事前の周知は、従業員等のアクセスログが知らない間にチェックされていたということがないようにする意味でも重要です(従業者のモニタリングを実施する上での留意点については、ｐ．○の「ｈ．外部へ送信するメールのチェック」の脚注を参照)。

○　ログの保存期限については、情報漏えいのリスクの高い情報に関するログか否か、ログの保存にかけられるコストはどの程度かといった観点を踏まえて決定することとなります。

○　なお、ログの確認を定期的に実施することで、情報漏えいにつながり得る兆候が把握できる場合があります。（詳細は第６章）

ｐ．秘密情報の管理の実施状況や情報漏えい行為の有無等に関する定期・不定期での監査

○　内部監査等を実施する際に、秘密情報の管理が適切に実施されているかを監査するとともに、資料の不足・欠損、不審な情報システムログ等の情報漏えい行為につながり得る兆候がないかを監査するとともに、監査が実施されている旨を周知します。

※監査の実施は、従業員等の秘密情報の取扱い方法等に関する認識を高めることにもつながります（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））。

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）」に資する対策

ここで紹介する対策は、

ａ．秘密情報の取扱い方法等に関するルールの周知

ｂ．秘密保持契約等（誓約書を含む）の締結

ｃ．秘密情報であることの表示

を行うことで、従業員等の秘密情報の対象範囲や取扱いについての認識を深め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」、「社外へ持ち出してはいけない情報だとは思わなかった」、「秘密を保持する義務を負っている情報だと思わなかった」といった言い逃れができないようにします。

ａ．秘密情報の取扱い方法等に関するルールの周知

○ 秘密情報の取扱い方法等に関する社内の規程等（本章３－３に記載）は、社内に周知しなければ、それを守るべき従業員等にその内容を認識させることはできません。そのため、社内の規程等の内容について、従業員等が認識できるよう、継続的に研修等を実施することが重要です。その際には、規程の内容のみならず、情報管理の徹底が自社の発展に貢献した事例や、社内で起こった秘密情報の漏えいとその結果に関する事例（「企業への帰属意識・信頼関係の向上等」に資する対策）といった具体的事例を取り上げながら、説明することも効果的です。

（本対策に必要な社内規程の条項）

- 社内規程の適用範囲
  : 役員、従業員、派遣労働者、委託先従業員（自社内において勤務する場合）等、本規程を守らなければならない者を明確にします。
- 秘密情報の定義
- 秘密情報の分類
  : 分類の名称（例えば「役員外秘」、「部外秘」、「社外秘」など）及び各分類の対象となる秘密情報について説明します。
- 秘密情報の分類ごとの対策
  :「秘密情報が記録された媒体に分類の名称の表示をする」、「アクセス権者の範囲の設定」、「秘密情報が記録された書類を保管する書棚を施錠管理して持出を禁止する」、「私物のＵＳＢの持込みを制限し複製を禁止する」など、分類ごとに講じられる対策を記載します。）
  （秘密情報の分類ごとの指定やその秘密情報へのアクセス権の付与実施する責任者について規定します。
- 秘密情報及びアクセス権の指定に関する責任者

:分類ごとの秘密情報の指定やその秘密情報についてのアクセス権の付与を実施する責任者について規定します。

- 秘密保持義務

:秘密情報をアクセス権者以外の者に開示してはならない旨などを規定します。

○ 研修等については、以下のような方法が考えられます。

（研修等の内容の例）

- 「秘密情報の管理の重要性」、「秘密情報の分類」、「秘密情報の具体的取扱い方法」を盛り込んだ資料を作成する。なお、社内規程等の変更があった場合にはそれを盛り込む。併せて、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）」に直接資する対策ではないものの、「秘密情報の管理の成功事例」、「秘密情報の漏えいとその結果に関する事例」、「関係法令の内容・改正状況」、標的型メールなどの警戒すべき手口とその対処方法等を盛り込んだ説明資料を作成しておくと効果的。

（研修等の実施の例）

- 定例の会議等での説明資料の配布、社内電子掲示板等への掲示、電子メールでの送付。
- 定期的に行われる朝礼や課内会議等での、秘密情報の取扱いに関する注意喚起・意識の共有。
- 入社時、昇進時等、定期的に実施される研修の講義内容として盛り込む。
- 守るべきルールの変更（関係法令や社内規定の改正等）に伴う研修の実施。
- 秘密情報の管理に関する研修会を実施（情報漏えいリスクや責務に応じて部門や役職ごとの研修会等の実施も効果的です）。
- 従業員等がいつでも受講できるよう、e-ラーニングを導入。理解度確認付 e-ラーニング等の従業員等全員の受講が確認できる教育プログラムの実施。

○ 研修等を実施した後に、例えば、「研修内容について理解したので、今後の情報の取扱いには注意します」といった誓約書を取ることは、従業員等の認識を更に深める対策として有効です（秘密保持契約等（誓約書を含む）の締結については「ｂ．秘密保持契約等（誓約書を含む）の締結）」に記載）。

ｂ．秘密保持契約等（誓約書を含む）の締結

○　従業員等に、自社の秘密情報の範囲等について認識させる方策として、社内の規程等に加え、又は規程に代えて、秘密情報を取り扱う従業員等と秘密保持に関する契約を締結したり、従業員等に対して誓約書を要請することが考えられます。

※規程等に加えて秘密保持契約を締結する場合は、秘密保持契約において、その規程の内容を引用し、規程を遵守することを義務として盛り込むという方法もあります。

○　秘密保持契約等は、従業員等個人が契約等の当事者になるため、その従業員等の秘密情報の管理に対する認識をより確実なものとする効果があります。

○　契約等に盛り込む内容として、「秘密を守る」という内容のみ規定した場合、退職時に社内資料を自宅に持ち帰ったまま返還しない、個人メールアドレスにメールを送信する等の行為は該当しないといった言い逃れを許すおそれがありますので、「持出禁止（持出が認められる場合はその条件）」といった取扱いの内容も定めておくことも考えられます。

○　秘密保持契約等を締結するタイミングとしては、入社時、退職時、在職中（部署の異動時、出向時、プロジェクト参加時、昇進時等の取り扱う情報の種類や範囲が大きく変更されるタイミング）等が考えられます。入社時の契約では、秘密保持義務の対象となる情報の特定は難しい場合が多いですが、在職中、退職時には、対象となる情報の範囲が徐々に容易になりますので、対象範囲をできる限り明確化した上で、秘密保持契約等を締結します。

○　また、「ａ．秘密情報の取扱い方法等に関するルールの周知」における研修等の実施の後に、「研修内容について理解したので、今後の情報の取扱いには注意します」といった誓約書を従業員等から取ることも、秘密情報の管理に係る認識を向上する対策として有効です。

ｃ．秘密情報であることの表示

ｉ）秘密情報が記載された媒体への表示

○　社内の規程に基づいて、秘密情報が記録された媒体等（書類、書類を綴じたファイル、ＵＳＢメモリ、電子文書そのもの、電子文書のファイル名、電子メール等）に、自社の秘密情報であることが分かるように表示を行います。

○ 表示は、社内の規程で定めた「秘密情報の分類」の名称を表示することが考えられます。その際、その表示を見た者が、その表示が付されている情報が、自社における秘密情報であることに加えて、アクセスできる者の範囲（例えば「役員限り」等）や、どのような取扱い方法（例えば「持出禁止等」）が求められている秘密情報であるのかも認識できるような表示とするとより効果的です。

○ また、秘密情報が記録された媒体等を保管する書庫や区域（倉庫、部屋など）に「無断持出し禁止」といった掲示を行うことも考えられます。

ⅱ）直接表示することが困難な物件等

○ 工場の生産ラインのレイアウトや金型等、そのもの自体に秘密情報であることの表示が困難なものについては、自社の秘密情報にあたる物件が保管されている場所に「無断持出し禁止」、「写真撮影禁止」といった掲示をしたり、物件リスト作成して、従業員等へと周知するといった方法が考えられます。

⑤「企業への帰属意識・信頼関係の向上等」に資する対策

ここで紹介する対策は、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。これらの取組によって、職場のモラルを維持することを目的としています。

【秘密情報の管理に関する従業員等の意識向上】

従業員等の、秘密情報の管理の重要性に関する理解を深め、漏えいに対する危機意識を高めることを目的とします。

ａ．秘密情報の管理の成功事例の周知

○ 秘密情報の管理等に係る研修等において、秘密情報の管理の徹底が、企業の発展・業績向上などに貢献したという事例を紹介して、秘密情報の管理の重要性に関する理解を深めます。

ｂ．情報漏えいの事例の周知

○ 秘密情報の管理等に係る研修等において、秘密情報の漏えいが企業に多大な損害を与え得るものであることについて、自社内外の具体的な漏えいとその結果に関する事例等[15]をまとめた資料や映像等を準備し紹介します。

ｃ．情報漏えい事案に対する社内処分の周知

○ 秘密情報の管理に係る研修等において、情報漏えい事案に対して、社内においてどのような処分がなされるのかについて、予め従業員等に説明しておくことで、従業員等の情報漏えい行為を未然に防止します。「b. の具体的な情報漏えいの事例」とともに説明するとより効果的と考えられます。

※社内処分については従業員等に対して過度な萎縮とならないような配慮が必要です。

【企業への帰属意識の醸成・従業員等の仕事へのモチベーション向上】

企業への帰属意識の醸成は、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が実施されているところですが、これらの取組が、情報漏えい対策としても有効であると考えられます。

---

[15] IPA「組織における内部不正防止ガイドライン」に内部不正事例が紹介されています(p.64 参照)。

ｄ．働きやすい職場環境の整備

○ 例えば、ワーク・ライフ・バランスの推進の観点から、長時間労働の抑制（適正な業務配分等）や年次休暇取得促進のための体制構築（労働時間の適正化、多様な休み方の提案等）、福利厚生の充実などを実施することにより、従業員等が働きやすい職場環境を整えて、企業への帰属意識を高めます[16、17]。

○ また、上司と部下、同僚同士がコミュニケーションを取りやすい職場環境を整えることも、企業への帰属意識を高めることに貢献します[18]。

ｅ．透明性が高く公平な人事評価制度の構築・周知

○ 従業員等の業務範囲、責任を明確にし、業務への貢献を多面的に評価して納得感の高い人事評価制度を構築して、従業員等の就労継続や昇進意欲を向上させることは、従業員等の仕事へのモチベーション向上につながります。

○ 従業員等の能力や希望等を踏まえて配属等の適正な判断を行うことも仕事への満足度やモチベーション向上につながります。

○ 新商品開発や生産効率化に資する発明、業務にかかるコスト削減への取組、日々の業務の改善など、創意工夫を行って企業に貢献した者などに対する表彰制度や報奨制度を導入することも、モチベーション向上に貢献します。

---

16 「働き方・休み方改善ポータルサイト」（厚生労働省：http://work-holiday.mhlw.go.jp/index.html）では企業の先進的取組等が紹介されています。また、『ワーク・ライフ・バランスの実現に向けた 「３つの心構え」と「10 の実践」』（内閣府：http://wwwa.cao.go.jp/wlb/research/kouritsu/pdf/3point10jissen-1.pdf）では、ワーク・ライフ・バランスに係る基本的な実践方法や事例等が紹介されています。

17 日本労働組合総連合会では、「働くことを軸とする安全社会の実現（http://www.jtuc-rengo.or.jp/kurashi/anshin_shakai/data/201507digest.pdf）」へのアプローチとして「ディーセントワークの実現（経済的・社会的に自立できる質の高い雇用とワーク・ライフ・バランスの実現）」の重要性を挙げています。

18 「あかるい職場応援団」（厚生労働省：http://no-pawahara.mhlw.go.jp/）では、良好なコミュニケーションと前提となるディスコミュニケーションの解消に参考となる様々な情報が紹介されています。

（２）退職者等に向けた対策

（退職者等とは）

自社を定年退職・中途退職した者（本人の意思に基づかない退職も含む）が典型的ですが、契約期間や実習期間が満了した派遣労働者や実習生など、自社内での勤務を終了した者を広く含みます。また、ここでは、退職の申し出があってから実際に退職するまでの間の者など（退職予定者等）も含みます。

退職者等は、元々は従業員等であることから、退職予定者等に対しては、従業員等に向けた対策を、必要に応じて一部の対策を強化しつつ実施し、実際に退職した後については、転職先等での行動を把握するといった特有の対策を実施することが考えられます。

①「接近の制御」に資する対策

ここで紹介する対策は、定年退職の場合は、しかるべきタイミングで、そして、中途退職の場合は申し出を受けた後速やかに、秘密情報へのアクセス権を削除する等の対策を講じることで退職までの間、秘密情報に近づけないようにすることを目的としています。

ａ．適切なタイミングでのアクセス権の制限

○ 退職時には、遅滞なく、その退職者の情報システムの利用者ＩＤやアクセス権限を削除します。加えて、確実にＩＤカードや会社への入館証を回収するとともに、当該ＩＤカード等では施錠された区域への解錠が出来なくなっていることを確認します。

○ 従事している業務内容によっては、退職予定者について、しかるべきタイミングで、秘密情報へのアクセス権を適切に制限することも考えられます。

②「持出し困難化」に資する対策

ここで紹介する対策は、退職予定者について、従業員等に対する対策に加え、その一部の対策をより厳格化したり、追加的な対策を実施する等して、秘密情報が記録された媒体等の社外への持出す行為を物理的、技術的に阻止することを目的としています。

【従業員等に向けた対策（再掲）】

（書類、記録媒体、物自体等（複製物を含む。）の持出しに対する措置）

ａ．秘密情報が記された会議資料等の適切な回収

ｂ．秘密情報の社外持出しを物理的に阻止する措置

ｃ．電子データの暗号化による閲覧制限等

ｄ．遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用

（電子データの外部送信による持出しを困難にする措置）

ｅ．社外へのメール送信・Ｗｅｂアクセスの制限

ｆ．電子データの暗号化による閲覧制限等

ｇ．遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用

（秘密情報の複製を困難にする措置）

ｈ．コピー防止用紙やコピーガード付の記録媒体・電子データ等により秘密情報を保管

ｉ．コピー機の使用制限

ｊ．私物のＵＳＢメモリや情報機器、カメラ等の記録媒体・撮影機器の業務利用・持ち込みの制限

【退職予定者に対する特有の措置】

Ⅰ．社内貸与の記録媒体、情報機器等の返却

○ 定年退職が近い者の場合は、従事させる業務内容も踏まえた適切なタイミングで、中途退職者については、退職の申し出を受けてから速やかに会社貸与の記録媒体や情報機器を返却させます。

※記録媒体、情報機器等の返却時には、その記録媒体や内部に保管された電子データ等に対して、利用者が設定したパスワードも提出させるようにします。

○ 必要に応じて、在職中に使用していたＰＣは回収し、実際に退職するまでは初期化されたＰＣを新たに貸与して残務に従事させるということも考えられます。

③「視認性の確保」に資する対策

ここで紹介する対策は、退職予定者については、従業員等に対する対策に加え、その一部の対策をより厳格化する、追加的な対策を実施する等して視認性を高め、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ことを認識させるようすることを目的としています。

また、退職者については、可能な範囲で転職先での行動等を把握するような対策を講じることが考えられます。

【従業員等に向けた対策（再掲）】

（管理の行き届いた職場環境を整える対策）

ａ．職場の整理整頓（不要な書類等の廃棄、書棚の整理等）

ｂ．秘密情報の管理に関する責任の分担

ｃ．「写真撮影禁止」、「関係者以外立入り禁止」の表示

（目につきやすい状況を作り出す対策）

ｄ．職場の座席配置・レイアウトの設定、業務体制の構築

ｅ．従業員等の名札着用の徹底

ｆ．防犯カメラの設置等

ｇ．秘密情報が記録された廃棄予定の書類等を従業員の目の届くところに保管

ｈ．外部へ送信するメールのチェック

ｉ．内部通報窓口の設置

（事後的に検知されやすい状況を作り出す対策）

ｊ．秘密情報が記録された媒体の管理等

ｋ．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

ｌ．印刷者の氏名等の「透かし」が印字される設定の導入

ｍ．秘密情報の保管区域等への入退室の記録・保存とその周知

ｎ．不自然なデータアクセス状況の通知

ｏ．ＰＣやネットワーク等の情報システムにおけるログの記録・保存とその周知

ｐ．秘密情報の管理の実施状況や情報漏えい行為の有無等に関する定期・不定期での監査

【退職予定者に対する特有の措置】

ｑ．退職をきっかけとした対策の厳格化とその旨の周知

○　現職の従業員等に向けた「視認性の確保」に資する対策について、退職の申し出等をきっかけとして、必要に応じて、例えば以下のような形で厳格化します。

（厳格化する対策の例）

- 「ｏ．ＰＣやネットワーク等の情報システムにおけるログの記録・保存とその周知」について、退職の申し出があった後だけでなく、以前のものも含めて、ログを集中的に確認する。

ｒ．ＯＢ会の開催等

○　例えば、ＯＢ名簿や中途退職者名簿の作成・定期的な更新を行ったり、ＯＢ会の開催を通じて退職者との定期・不定期の交流機会を持ったりすることで、退職者の動向の把握に努めていることを認識させることが考えられます。その他、同期会などにおいて中途退職者の近況について情報が得られる可能性もあります。

○　また、退職後も一定の交流を保つことは、退職者等の自社に対する愛着を高め、企業への帰属意識の継続につながる場合もあります。

○　一方で、ＯＢ会に現役社員も参加する場合には、ＯＢが現役社員から最新の情報を得る良い機会になってしまうこともありますので、参加する現役社員への予めの注意喚起が重要です。

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）」に資する対策

ここで紹介する対策は、退職予定者に、漏えいしてはいけない自社の秘密情報について、再度確認等することで認識を高めることを目的としています。これにより、同時に、退職時に情報漏えいを行った者が「秘密情報であることを知らなかった」等の言い逃れができないようにすることも目的としています。

ａ．秘密保持契約等の締結

○ 特に退職後時には、改めて明確な注意喚起を行うべく、就業規則等による一般的な秘密保持義務に係る規程の有無にかかわらず、退職者と、個別に秘密保持契約等を締結することが重要です。

○ 秘密保持契約等の締結に当たっては、退職者予定者との面談等を通じて、在職中にアクセスした秘密情報を確認し、それらが秘密保持義務の対象に含まれるように秘密保持義務を設定します（加えて、その面談の内容も客観的な形で記録を残すことも考えられます）。

※なお、退職時に突然契約の話をされると、退職者が当惑する可能性があることから、退職時に秘密保持契約を締結する場合があることを事前に周知しておくと、よりスムーズに契約締結の手続を進められるでしょう。

ｂ．競業避止義務契約の締結

○ 退職者のうち、例えば重要なプロジェクトにおけるキーパーソンなど、自社の利益を守るために秘密保持義務をより実効的にすることが必要だと考えられる場合、競業避止義務契約を締結することも考えられます。

○ しかし、競業避止義務契約は、秘密保持契約と異なり、より直接的に「職業選択の自由」を制限するおそれがありますので、労使相互において、その必要性や内容の十分な理解を図るとともに、義務範囲を合理的なものとすることが重要です。

※なお、退職時に特有の契約の一つとして、ここで競業避止義務について紹介していますが、競業避止義務契約は、秘密保持義務をより実効的にするものであるため、この契約自体が直接的に「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）」に資する対策ではないことに留意が必要です。

ｃ．秘密情報を返還・消去すべき義務が生ずる場合の明確化等

○ 退職時に締結する秘密保持契約において、秘密保持義務の対象となる情報が記録された資料や記録媒体を返還するとともに、電子データについては消去し、その情報を自ら一切保有しないことを確認するといった契約条項を盛り込み

ます。

○　この対策により、退職者等が、返還・消去すべき情報を認識できるようにします。また、返還・消去義務に違反した者が、「返還・消去すべき情報だとは思わなかった」、「返還・消去したと言った覚えはない」といった言い逃れ訳をすることを防ぐことも可能となります。

⑤「企業への帰属意識・信頼性の向上等」に資する対策

ここで紹介する対策は、適切な退職金の支払い、ＯＢ会の開催等により、退職者等の自社への帰属意識の継続をさせること等を目的としています。

ａ．適切な退職金支払い

○　退職金制度を設けている場合には、法令に従い、就業規則等により、適用される従業員等の範囲や退職手当の計算方法、支払い方法、支払い時期等を予め明確にしておき、それに基づいた適切な退職金の支払いを実施することにより、円満な退職を促し、自社への帰属意識を維持するようにします。

ｂ．退職金の減額などの社内処分の実施

○　競合他社に再就職する等、退職後において情報漏えいを行う可能性が高いと認められる場合には、退職金の減額処分や返還請求などが実施されることを予め社内に知らせておき、それを現実に実施することで、退職者の漏えいに対する危機意識を高めます。

ｃ．ＯＢ会の開催等（再掲（「視認性の確保」））

○　例えば、定期的なＯＢ会の開催を通じて、退職者との定期・不定期の交流機会を持ったりすることで、退職者等の自社に対する愛着を高め、企業への帰属意識を継続させるようにします。

○　キーパーソンについては、一旦退職した後も、改めて秘密保持義務契約を締結した上で、「非常勤顧問」等として再雇用することも考えられます。

（３）取引先に向けた対策

（取引先とは）

○ 自社の秘密情報を共有する相手方を指します。例えば、委託先や委託元、外注先や外注元、共同研究相手などが考えられます。

※自社内で業務を行う委託先従業員については、（１）従業員等に向けた対策の対象となります。

（ここで紹介する対策）

○ 取引先を通じた情報漏えいの中には、大別して、以下の２つのパターンが考えられます。

（ⅰ）取引先自体が主体となり悪意で情報の不正使用や不正開示を行う場合

（ⅱ）取引先の情報管理が不十分であったことに起因して、相手方従業員、退職者、再委託者や外部者等を通じて情報漏えいしてしまう場合

○ 上記（ⅰ）に関しては、取引先に対して自社が直接情報漏えい対策を実施する必要があり、（ⅱ）に関しては、取引先の社内での情報漏えい対策の実施を、当該取引先に対して要請することが考えられます。

○ ここでは（ⅰ）に係る対策のみを紹介しています。（ⅱ）については、自社内で実施する対策の水準等を参考に、必要と考えられる対策を取引先に実施させるという観点から、契約内容等を検討することが重要です。

（取引を開始する前に留意すべき点）

○ 取引先への対策を検討する前提として以下の２点について留意することが重要です。

- 秘密情報を取り扱う業務を不用意に委託しない

  秘密情報を取り扱う業務について委託等を検討する場合、予め、その委託等により生ずるリスクを考慮し、真に必要な取引であるかを検討する必要があります。例えば、コストを安く抑えられるからという理由だけで海外の取引先に不用意に秘密情報を取り扱う業務を委託してしまうと、物理的に管理が行き届かないばかりでなく、法律や商慣行の違い等により漏えいリスクが高まる可能性もあります。

- 取引先の管理能力の事前確認

  取引先の決定に当たっては、当該相手方が秘密情報を適切に管理し、かつ、自社からの情報管理に係る要請に適切に対応できる能力を有するか否かを、事前調査や、ＩＳＭＳ（情報セキュリティマネジメントシステム）などの基準・認証・

資格などを参考としつつ、事前に確認することが重要です。

○　以上の２点を踏まえ、取引先に秘密情報を共有することを決定した場合、取引先に向けた対策として、以下を検討します。

①「接近の制御」に資する対策

ここで紹介する対策は、取引先に対して、極力、秘密情報に接触する者を少なくし、権限のない者を秘密情報に近づきにくくすることを目的としています。

ａ．取引先に開示する情報の厳選

○　取引先に秘密情報を開示して事業を遂行することを決定した場合には、契約の前後に関わらず、それぞれの秘密情報について、開示の必要性を慎重に判断し、開示する秘密情報を必要最低限に厳選することが重要です。

具体例

- 契約前の商談等の場においては、秘密情報が記載された資料は渡さず、その場で回収したり、コアな情報は伝えないよう徹底する。
- コア技術に係る特に重要な秘密情報は取引先に開示せず、周辺技術のみ開示し、その範囲のみでの業務委託にする。
- 複数の委託先に業務を分担させた上で情報を渡す事で、特定の取引先に情報が集中しないように配慮する。
- 取引先が自社に来訪する場合でも、書庫や工場等への不必要な立入をさせないようにする。
- 契約の範囲外の情報を渡さないよう徹底する。

ｂ．取引先での秘密情報の取扱者の限定

○　取引先において、秘密情報の取扱者が不必要に増えると、その分管理が行き届きにくくなり、漏えいのリスクが高まると考えられます。したがって、取引先において秘密情報を取り扱う者を限定することが重要です。

具体例

- 契約書等において、取引先における秘密情報の取扱者を指定する。その際、取扱者を変更する場合には、自社の許可が必要である旨契約書に規定する。
- 契約後の秘密情報のアクセスについては自社サーバーを利用することとし、そのアクセス権限を自社で管理する。（その際、サーバーへのアクセスログを記録・確認することは、③「視認性の確保」にも資するものと考えられます。）

②「持出し困難化」に資する対策

取引先に秘密情報を共有・開示する場合には、自社サーバーの利用等を除き、既に秘密情報を物理的に自社外に出しているため直接の管理が及ばず、不正な持出しを困難にする対策は基本的に考えられません。したがって、①「接近の制御」に記載した対策を中心に、その他の目的に資する対策を確実に実施することが重要です。

ａ．秘密情報の消去・返還と複製できない媒体での開示

○ 契約満了時や契約解除時に相手方が自社の秘密情報をそのまま持ち続けてしまうことのないよう、委託契約や秘密保持契約等に、秘密情報の消去義務を設け、併せて、消去した旨の報告義務や消去の証明義務を設けることが有効と考えられます。

○ この実効性を確保するためには、複製ができない媒体（コピー防止用紙やコピーガード付のＵＳＢメモリ、ＣＤ－Ｒ等）や、文書作成ソフトの一般的な機能などを活用し、コピー・印刷や記録媒体への記録を禁止する設定を施した電子データを用いることも考えられます。

○ 業務の委託等にあたり、取引先に対して自社が直接管理できるサーバーを使用させた場合、そのサーバー内のデータのダウンロードや印刷等を禁止する設定とするなど、取引先が実施できる操作を必要最低限にすることが有効です。

ｂ．遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用

○ アクセス権者の頻繁な変更を自社で直接コントロールしたり、契約満了後等に、万一ＰＣやデータが取引先に残った場合に備え、以下の市販のツールやサービスを利用することも考えられます。

具体例

- 遠隔操作によりＰＣ内のデータを消去できるツール。
- 情報機器について、パスワードロックによる認証を設定し、一定回数、認証に失敗すると重要情報を消去するツール。
- 一定期間、管理サーバーとのやり取りがなされない状態が続いた場合に指定したデータが自動的に消去されるサービス。
- 電子データそのものに遠隔操作による消去機能を備えさせるツール。

③「視認性の確保」に資する対策

ここで紹介する対策は、取引先について視認性を強化し、秘密情報を漏えいしたとしても見つかってしまう可能性が高い状態であることを認識させることを目的とします。また、こうした取組を強化することにより、互いの状況をよく把握できるようになり、情報漏えいの疑いが生じた場合等にも、客観的事実に基づいて判断できるため、無用なトラブルを避けることにもつながります。

ａ．秘密情報の管理に係る報告の確認、定期・不定期での監査の実施

○ 取引先に対し、秘密情報の管理に係る義務の履行状況を報告させ、その内容が契約内容に沿うものか否かを確認したり、定期・不定期に秘密情報の管理状況の監査を実施することにより、その管理を確実なものとするとともに、不正行為をしたとしても見つかってしまう可能性が高い状態であることを認識させることができます。

具体例

- 契約等に、秘密情報を管理していることを定期的に報告する義務を定め、その報告が契約内容に沿うものか否かを確認する。
- 契約等に、定期的に秘密情報へのアクセスログを提出させる義務を定め､アクセス者やその閲覧頻度等が契約内容に沿ったものか否か確認する。
- 契約等に秘密情報の管理状況について監査を実施する旨を規定し、定期・不定期に情報管理体制やその履行状況の監査を実施する。

ｂ．取引先に自社サーバーを使用させてログの保全・確認を実施

○ 個人情報など、漏えいした場合に他者に被害を与えるような情報の場合や、多数の者により管理・活用される情報など、特に取引先の視認性を確保する必要があると考えられる場合には、自社が直接管理できるサーバーを使用することを条件とした委託契約等を締結し、そのログを確認することが考えられます。なお、その際、当該サーバーは、一定のセキュリティレベルが保たれていることが前提です。

④「秘密情報の認識向上（不正行為者の言い逃れの排除）」に資する対策

ここで紹介する対策は、取引先に対し、漏えいしてはいけない秘密情報を明示し、その認識を深めることを目的としています。また、それにより取引先が情報漏えいを行った際に「秘密情報であることを知らなかった」等の言い逃れができないようにすることも目的としています。

ａ．取引先に対する秘密保持義務条項

○ 取引先に対し、自社が開示する情報が秘密情報であり、取引先にとって秘密保持の対象になるということを示すため、取引開始時に、秘密保持の対象となる情報をできる限り明確化した秘密保持契約等を締結することが必要です。

○ たとえば、リスト化や文書化による情報の明確化にあたり、その記載を「○○で開示されたすべての情報」などとしてしまうと、事業を実施する中で、公知情報等を混在して開示してしまうこと等により、秘密保持の対象が不明確になる懸念があるため、以下の具体例を参考に、その対照を明確化することが有効です。なお、当該契約は、必要や状況に応じて見直すことも考えられます。

具体例

- 契約等において、秘密保持の対象を「基本契約又は個別契約により知り得た相手方の営業上又は技術上の情報のうち、相手方が秘密である旨明示したもの」とし、実際の秘密情報の受渡しに際して秘密であることを明示する。
- 契約書等において、「甲が乙に秘密である旨指定して開示する情報は、別紙のとおりである。なお、別紙は甲乙協力し、常に最新の状態を保つべく適切に更新するものとする。」旨記載し、双方協議の上、秘密保持の対象情報をリスト化し、リストは常に最新の状態を保つよう更新する。
- 委託契約等の事業開始後に事前の契約等において指定した情報の範囲を超えるものを口頭で開示した場合には、開示した側が、情報の開示後一定期間内に当該情報の内容を文書化し、当該文書を秘密保持義務の対象とすることとするなど、予め口頭で開示した情報の取扱いに関する規定を設ける。

ｂ．秘密情報であることの表示

○ 実際に秘密情報に接する取引先の従業員の認識をより確実にするためには、取引先に開示する紙媒体の資料やファイル、ＵＳＢメモリ、ＣＤ－Ｒ等の記

録媒体、電子データ等に「秘密情報」であることの表示をすることが重要です。

c．具体的な秘密情報取扱い等についての確認

○ 取引先の従業員等が、秘密情報について不適切な取扱いをすることのないよう、取引先が実施する秘密情報の具体的管理方法を事前に確認した上で、それを契約書に定めることが有効です。

d．取引先に対する秘密情報の管理方法に関する研修等

○ 取引先での秘密情報の認識を確実にするため、契約における具体的な秘密情報の対象やその管理方法について研修等を実施することが有効です。なお、④「秘密情報の認識向上（不正行為者の言い逃れの排除）」に直接資する対策ではないものの、標的型メールなどの警戒すべき手口とその対処方法についても、併せて研修や訓練を実施することで、取引先に対する外部者からの不正アクセス行為等を通じて、自社の情報が漏えいしてしまうことを防ぎます。

e．取引先とのやりとりの議事録等の保存

○ 取引先に対し、秘密情報を開示するに当たり確認した事項や決定した内容について、それを記録として残すことは、取引先に秘密情報を授受したことを認識させるために有効です。

具体例

- 秘密情報の特定に当たって行う協議等のやりとりは、双方合意の上議事録を作成する。
- 秘密情報の授受に当たり、それを台帳で共有管理する（秘密情報の内容、授受の日時、保管場所、提供先等）。
- メールで秘密情報の授受を実施した場合にはそのメールでのやり取りを保存しておく。

⑤「企業への帰属意識・信頼関係の向上等」に資する対策

ここで紹介する対策は、取引先と自社との信頼関係を向上させることを目的としています。

ａ．適正な対価の支払い等

○ 関係法令や各種ガイドライン等を遵守し、取引を適正化して取引先と公正で円満な関係を築くことは、取引先が不正を起こすきっかけとなり得る環境を作らないための基本的な前提となります。

具体例

- 親事業者と下請事業者の関係の場合には、「下請適正取引等の推進のためのガイドライン」[19]を参考にして、価格協議を頻繁に実施して原材料価格等の高騰分を適切に取引価格に反映するなどの対応をする。
- コンプライアンス宣言等を作成・公表し、それに基づいて相手との関係を構築する。
- 公平な取引を推進するため、自社従業員に向けた倫理研修を実施する。

ｂ．契約書等における損害賠償や法的措置の記載

○ 取引における契約書等において、秘密保持義務の違反時における損害賠償の責任を規定したり、契約時に、秘密情報の漏えい等に対して自社が法的措置等の厳正な処置をとることを明記した自社のポリシーを通知すること等は、取引先による情報漏えいを牽制する効果があります。

19「下請適正取引等の推進のためのガイドライン」 業種別一覧
http://www.chusho.meti.go.jp/keiei/torihiki/ShitaukeGuideLineGyoushu.htm

（４）外部者に向けた対策

（外部者とは）

基本的には上記（１）従業員等、（２）退職者等、（３）取引先以外の者をいいます。例えば、工場への不法侵入者やサーバーへの不正アクセス行為者が該当します。また、そのような悪質性の高い者だけでなく、自社への来訪者（各種渉外販売員、工場見学者等）、各種メンテナンス業者など自社への立入りが許されている外部者も含まれます。

（留意点）

外部者に対しては、基本的に「⑤企業への帰属意識・信頼関係の向上等」に係る対策は有効ではなく、また、「④秘密情報の認識向上（不正行為者の言い逃れの排除）」に係る対策も有効でない場合が多いと考えられます。したがって、特にそれ以外の「①接近の制御」、「②持出し困難化」、「③視認性の確保」の対策を中心に対策を検討することが必要です。

①「接近の制御」に資する対策

ここで紹介する対策は、外部者を秘密情報に極力近づけないことを目的としています。

外部者に対しては、この「接近の制御」に資する対策を確実に行うことが最も重要です。

ａ．秘密情報を保管する建物や部屋の入場制限、書棚や媒体等のアクセス制限

○ 秘密情報を保管する建物や部屋等については、許可された者以外は入場、入室等できないよう制限することが重要です。

具体例

- 秘密情報を保管する社屋の施錠管理（アクセス権を持たない者がアクセス権者といっしょに入構することを防止する観点から、防犯カメラの併設が望ましい）。
  ex）執務室には近づけないオフィスの設計（来訪者は玄関に設置された内線電話により、従業員を呼び出し内側から解錠してもらわなければ入構できない工夫、執務スペースを通らなくても応接スペースを利用できるようなレイアウトの工夫等）。
- 敷地入り口での警備員による身分確認。
- 入構ゲートの利用によるＩＤでの入構制限。
- 書類・ファイル、記録媒体を書棚や区域（倉庫、部屋など）に保管し施錠管理。

○ 各種メンテナンス業者等、物理的に社屋内等で活動する外部者に対しては、社屋への入構は一般的に許可されているため、入室できる場所を限定したり、秘密情報を管理する書棚やＰＣ、ＵＳＢメモリ等の記録媒体自体に制限をかけることが有効です。それらは、持ち出されてしまった場合にも有効な取組（持出し困難化）であることがあります。

具体例

- 秘密情報を保管した書棚の施錠管理。
- ＰＣのＩＤ、パスワードによる認証管理。
- ＵＳＢメモリ等の記録媒体のパスワード管理。

ｂ．外部者の構内ルートの制限

○ 工場の視察や見学を受け入れる際には、そのルートを適正に限定し、秘密情

報が保管されたエリアや部屋には近づけないようにすることが有効です。

具体例

- それ自体が秘密情報である製造機械等は見学ルートに含まない。
- 見学者の通るルート沿いには秘密情報を放置しない。
  - ex）秘密情報が表示された物件にカバーをかける。
  - ex）秘密情報が保管されたサーバールームや書庫等については、フロアマップや部屋の表札等にはそれと分かる記載をしない。

ｃ．ペーパーレス化

○ 自社内の秘密情報をペーパーレスにすることは、オフィスへの来訪者等が秘密情報に接する機会を少なくするため、外部者の秘密情報への接近の制御に非常に有効です。その際、併せて電子化された秘密情報へのアクセス制限を実施することが望まれます。加えて、電子化された秘密情報について、印刷やコピーができない措置を施すことで②「持出し困難化」にも資することになります。なお、完全なペーパーレス化を実施することが難しい場合でも、電子化された秘密情報について､印刷できるデータの内容や､印刷できる者、印刷の目的等を限定するというルールを設け、併せてその印刷物の廃棄方法にも留意することで、同様の効果が得られます（廃棄方法についてはｄ．に記載）。

ｄ．秘密情報の復元が困難な廃棄・消去方法の選択

○ 秘密情報が記録された書類・ファイルや記録媒体等の廃棄、秘密情報が記録された電子データの消去を行う場合、外部者が、廃棄・消去された情報を復元して、その情報にアクセスすることができないように、以下のように復元不可能な形にして廃棄・消去します。

（具体的な廃棄・消去方法）

- 書類の廃棄方法
  - ex）シュレッダーにより裁断し、廃棄。
    - ※秘密情報の重要度に応じて、より復元を困難とするため、クロスカット（縦方向と横方向の両方から裁断する）方式のシュレッダーを利用するなど、かけることができる費用の多寡も踏まえながら、シュレッダーの機能性について検討することも重要。
  - ex）秘密情報を廃棄するゴミ箱は、廃棄後取り出すことができない鍵付きゴミ箱に限定。
  - ex）重要度の高い情報等については、信頼できる専門処理業者に依頼し

て焼却・溶解処分。場合によっては、その証明書を発行してもらう。

- 秘密情報を保存していた記録媒体（ＵＳＢメモリ等）、ＰＣ、サーバーの廃棄方法

  ex）市販されている完全消去するソフトや、磁気記録方式のハードディスク磁気破壊サービス等を利用してデータを消去の上、その記録媒体等を物理的に破壊（記録媒体からデータを消去しただけでは復元されるおそれがあるため）。

ｅ．秘密情報を保管する機器を外部ネットワークから遮断

○　不正アクセス等に備え、その秘密情報の利用態様を踏まえ、ネットワークに接続された機器で利用・保管する必要性のない秘密情報については、その秘密情報を保管する機器をネットワークから遮断した状態にすることが有効です。

ｆ．ファイアーウォール、アンチウィルスソフトの導入、ソフトウェアのアップデート

○　ネットワークにつながったＰＣ等の機器に保管されている秘密情報を不正アクセス等から守るためには、ファイアーウォールの導入や、ウィルスに感染させないためのアンチウィルスソフトなどのセキュリティソフトの導入、各種ソフトウェアの適時のアップデートが重要です。さらに不正侵入防御システムの導入等により防御することも有効と考えられます。

○　外部者からの標的型攻撃などによる情報窃取活動の対抗手段としては、まずは社内における秘密情報へのアクセス権者を最小限にする対策が有効となります。したがって、本章３－４　（１）　従業員等に向けた対策　①「接近の制御」　を確実に実施することが有効です。

ｇ．ネットワークの分離（複数のＬＡＮを構築）

○　ネットワークを分離することで、１つのネットワークに不正アクセス等があった場合でも、その他のネットワークに保管される秘密情報へは直接アクセスできないため、接近の制御の強化とともにウィルス等に感染した場合でも被害の拡散防止にもなります。

②「持出し困難化」に資する対策

ここで紹介する対策は、外部者が仮に秘密情報にアクセスしたとしても、それを持ち出す行為を物理的、技術的に阻止することを目的としています。

ａ．外部者の保有する情報端末、記録媒体の持込み・使用等の制限

○ 各種メンテナンス業者や見学者等が秘密情報を保管する場所に入場する場合には、秘密情報を記録等できる機器（ＰＣやＵＳＢメモリ等）や撮影機器（カメラ等）の持込みを制限することが有効です。その際、荷物を預かったり、実際の見学に自社の担当者が付き添う等の取組を併せて行うことで、より実効性が向上すると考えられます。

○ 不正侵入者等による不正な複製等を制限するためには、ＰＣ等の機器に対する記録媒体の使用制限を実施することが有効です。

具体例

- ＵＳＢメモリの差込口がないものや、ＵＳＢメモリの差込口を無効化したり、物理的にふさぐ部品を取り付けたＰＣを利用する。
- 許可された会社貸与のＵＳＢメモリ以外は、ＰＣが認識しないよう設定する。

ｂ．ＰＣのシンクライアント化

○ データの保存といった機能をＰＣから切り離してサーバーに集中させ、ＰＣ自体には秘密情報を保管しない（ＰＣをシンクライアント化する）ことで、万が一ＰＣが盗難された場合にも秘密情報は持ち出すことができなくなります。

ｃ．秘密情報が記載された電子データの暗号化

○ 秘密情報が記載された電子データを暗号化しておくことによって、たとえ電子データが不正に持ち出されてしまっても、複合のためのキー（パスワードなど）がなければ解読できない状態とします。

ｄ．遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用

○ 万一、ＰＣやデータが盗難された場合に備え、以下の市販のツールやサービスを利用することも考えられます。

具体例

- 遠隔操作によりＰＣ内のデータを消去できるツール。

- 情報機器について、パスワードロックによる認証を設定し、一定回数、認証に失敗すると重要情報を消去するツール。
- 一定期間、管理サーバーとのやり取りがなされない状態が続いた場合に指定したデータが自動的に消去されるサービス。
- 電子データそのものに遠隔操作による消去機能を備えさせるツール。

③「視認性の確保」に資する対策

ここで紹介する対策は、外部者に対する視認性を強化し、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ことを認識させるようにすることを目的とします。

ａ.「関係者以外立入り禁止」や「写真撮影禁止」の張り紙等

○ 秘密情報が保管されている書棚や区域（倉庫、部屋など）に、「関係者以外立入り禁止」等の張り紙や看板を設置することで、外部者の出入りに対する従業員等の関心が高まるとともに、外部者に対して情報管理に係る関心が高く、管理が行き届いた職場であると認識させることで、不正な立入りや情報漏えい行為を心理的に抑止する効果が期待できます。

※なお、「関係者以外立入り禁止」等の掲示の際には、同時に「入室に関する問合わせ先」も記入しておかないと、「立入り禁止とは分かっていたけれど、担当者を探して入室してしまった」といった言い逃れを許してしまいかねないことから、より心理的な抑止効果を高めるため、「関係者以外立入り禁止」の看板には、管理者の連絡先も併記することが有効です。

ｂ．秘密情報を保管する建物・区域の監視

○ 秘密情報が記録された書類・記録媒体が保管・蔵置された建物や区域（倉庫、部屋など）、書棚、秘密情報の廃棄場所など、秘密情報の不正な取得や複製の現場となり得る場所について、以下のような方法により、不正行為が「目撃されやすい」状況とします。

具体例

- 秘密情報が保管された場所や、その出入口が、従業員等の死角とならないようにレイアウトを工夫する。その上で、出入口の扉の開閉時にはチャイムやブザーがなるよう設定し、人の出入りが、人目に立つ状態にする。
- 出入口での守衛による入退状況のチェック。
- 防犯カメラの設置。
- 入退室をＩＤカード等により制限し、その入退室のログを保存、確認

○ 不正アクセス等に備え、ＰＣやネットワーク等の情報システムにおけるログを記録・保存、確認することも重要です[20]。

[20] 特に近年その巧妙さを増す標的型攻撃への対策の際に参考となるものとして、自社のシステム内部に深く侵入してくる高度な標的型攻撃を対象に、システム内部での攻撃プロセスの分析と

具体例

- ファイアーウォールのログなどの外部からの通信に係るログ（ファイアーウォールの透過や拒否のログなど）や、ＰＣ等のアクセス履歴に係るログ等を記録・保存し、定期的に確認します（さらに、組織内から外部に向けた通信ログも保存して定期的に確認をすれば、万が一標的型攻撃等によりウィルスに感染し、社内の秘密情報が外部に送信された場合にも、速やかに発見することが可能になります）。

○ 特に、各種メンテナンス業者等、外部業者などの、一定の社内における活動を許された者に対しては、それぞれの業者の担当者を決め、外部業者の活動内容や人員の配置等について定期的に報告させ、把握していない活動を実施していないか確認します。（従業員の誰も何も知らないという状況で外部者が作業している状態をなくす。）なお、これらの取組は、事案が発生した場合の客観的な証拠となるため、取引先に対する無用な疑いを避けることにもつながります。

具体例

- 入構の事前届出をさせたり、社内活動に係る日報等を提出させる。
- 機器のメンテナンス事業者が来室する際には、必ずそのメンテナンス作業に立ち会う。
- 外部業者であることが外見上明らかな状態にするため、社内では制服を着用することを契約において規定。
- ＰＣの作業画面の録画や作業ログを残す。

○ また、秘密情報が保管される執務室等に外部業者などが立ち入る際には、執務室にいる従業員に対してそれを知らせることにより、秘密情報を放置したり、不用意に秘密情報を口にしてしまうことを防ぐことができます。

具体例

- 従業員への一斉メールで外部者の入室スケジュールを事前に周知する。
- 外部者が入室した場合にアラートやチャイムが鳴ったり、赤色灯が回るようにする。

内部対策をまとめた『「高度標的型攻撃」対策に向けたシステム設計ガイド』があります（(独)情報処理推進機構（IPA））。（https://www.ipa.go.jp/security/vuln/newattack.html）

ｃ．来訪者カードの記入、来訪者バッジ等の着用

○　自社の従業員でない者が執務室等に立ち入る場合には、入り口にて来訪者カード等を準備し、氏名や訪問先を記入してもらい、アポイントの有無を確認するなどにより、来訪者に対し、情報管理に係る関心が高く、管理が行き届いた職場であると認識させ、不正行為を心理的に抑制します。また、来訪者の入構時には、当該来訪者と実際に面識のある従業員が直接入口に出迎えることによって、来訪者のなりすましを防ぎます。

○　入構の際に、来訪者用のバッジ等を渡して着用してもらうことで、その者が来訪者であるということが外見上明らかとなり、従業員等の意識的又は無意識的な関心を集め、不正行為に対して心理的な抑止効果が期待できます。その際、来訪目的先ごとに色分けしたバッジ等を配布し、来訪目的の場所以外に立ち入った場合に人目に立つ状態とすることも有効です。（同時に、従業員等の社員証着用を徹底させ、社員証やバッジ等を「何も着用していない」ことが人目に立つ状態とすることにより、バッジ等を外されてしまう事態に備えることが考えられます）。

④「秘密情報の認識向上（不正行為者の言い逃れの排除）」に資する対策

ここで紹介する対策は、外部者が情報漏えいした際に「秘密情報であるとは気がつかなかった」等の言い逃れをできないようにすることを目的としています。ただし、外部者のうち、不法侵入者や不正アクセス行為者など、悪質性の高い者に対しては、基本的にはこれらの対策は効果が乏しい場合が多いと考えられますので、それらの者に向けた対策は、特に「①接近の制御」、「②持出し困難化」、「③視認性の確保」に資する対策を強化することが必要と考えられます。

ａ．「写真撮影禁止」、「無断持出し禁止」や「関係者以外立入り禁止」の張り紙等（再掲）

○ 不正行為者の言い逃れを排除する観点からは、特に各種メンテナンス業者等の何らかの契約に基づいて、その業務の為に執務スペースに立ち入ることが出来る者や、アポイントメントや渉外活動で立ち入る者に対しては、秘密情報が保管されている場所の入り口、書棚、作業場等に「写真撮影禁止」、や「関係者以外立入り禁止」「無断持出し禁止」等の張り紙や看板を設置することが有効です。

※なお、「関係者以外立入り禁止」の看板を掲げる時には、同時に連絡先も記入しておかないと、「立入り禁止とは分かっていたけれど、担当者を探して入出してしまった」という言い逃れを許してしまいかねないため、「関係者以外立入り禁止」の看板には、管理者の連絡先も併記することが必要です。

ｂ．秘密情報であることの表示

○ 外部者以外への対策と同様、実際に秘密情報に接した者が、その情報が秘密情報であることを認識できるようにするため、外部者が接する可能性のある紙媒体の資料・ファイル、ＵＳＢメモリ、ＣＤ－Ｒ等の記録媒体、電子データ等には、秘密情報であることを表示することが望ましいと考えられます。

※秘密情報の窃取を企図して不法侵入や不正アクセスなどを行う外部者に対しては、秘密情報であることを表示することによって、かえってそれと分かりやすくなってしまうという懸念もありますが、従業員等に向けた対策としては重要な対策であることや、来訪者や見学者等の悪意のない外部者が秘密情報と分からずうっかり持ち出してしまう懸念を考慮すれば、やはり表示しておいた方が望ましいと考えられます。その上で、不法侵入者等に対しては、「①接近の制御」、「②持出し困難化」、「③視認性の確保」などの取組を着実に行うことが必要でしょう。

ｃ．契約等による秘密保持義務条項

○ 各種メンテナンス業者等、一定の許可の下に、秘密情報に接する可能性のある事業者に対しては、「業務中に接する一切の情報を漏えいしてはならない」

旨を業務委託契約等に盛り込むこと等が重要です。

⑤「企業への帰属意識・信頼関係の向上」に資する対策

不法侵入や不正アクセスを企図する外部者に対しては有効な対策は考えにくいですが、一定の契約関係のある外部者に対しては、（３）取引先に向けた対策 ⑤「企業への帰属意識・信頼関係の向上等」の対策が有効な場合が考えられます。

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。

○ 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。

○ 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、下記の例を参考に、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[21]。

（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

21 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）47 ページ以下において、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）

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

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●「情報管理規程のひな形」を参照）

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、社外持ち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。

（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。

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の実施、監視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、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。
- 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

第５章　他社の秘密情報に係る紛争への備え

- 他社の秘密情報に係る紛争に巻き込まれてしまった場合に備えて、各企業においては、平時より適切な対策を講じておくことが重要です。
- 本章では、健全に事業活動を行っている企業が、図らずも紛争に巻き込まれてしまった場合に、正当にその立場を守ることができるようにするため、自社の保有する情報が真に独自のものであると立証できるようにしておくための日頃からの管理手法や、他社の秘密情報を意図せず侵害しないための予防策を紹介します（後者については、自社情報と他社情報の混在が起こりやすい場面ごとに紹介します）。特に、転職者の受入れや共同・受託研究開発における対策は、第１章で述べたとおり、人材の流動性の向上を通じた多様な人材確保やオープンイノベーションの更なる進展にも寄与するものと考えられます。
- また、平成２７年不正競争防止法改正により新たに規制対象となった営業秘密侵害品の取引について、紛争を防止するための方策も紹介します。

５－１　自社情報の独自性の立証

○　秘密情報の侵害を行ったとして、他社から不正競争防止法違反や契約違反等を理由とした損害賠償請求や差止請求訴訟を提起された場合等に、問題となっている情報が自社の独自情報であることを客観的に立証し、正当に自社の立場を守ることができるようにするため、平時より対策をしておくことが重要です。

○　こういった訴訟が提起されるリスクは、健全に事業活動を行っている企業であっても存在することに留意が必要です。例えば、自社製品と同じ機能・性能を持った製品を製造・販売している競合他社から提訴される、ライバル企業から嫌がらせ目的で提訴される、といったケースがあり得るところです。

○　また、例えば、何者かにより、他社から盗まれた営業秘密を示された場合に、それが盗まれた営業秘密であることを知らなかったとしても、知らないことにつき「重大な過失がある」（取引上の注意義務の著しい違反がある）と評価されるときには、不正競争防止法上、その営業秘密を取得する行為等が損害賠償請求や差止請求の対象となり得ます（不正競争防止法第２条第１項第５号等）。自社情報の独自性の立証に万が一失敗し、このような訴訟に敗訴してしまうと、関連事業の停止や風評被害による業績の悪化といった多大なる損失が発生することとなります。

具体例

（基本的な考え方）

- 情報の作成・取得過程、更新履歴、可能であれば消去された日時・内容のログ等について、関係する資料（電子メール、検討文書、メモ、議事録等）を保管する。その際、ファイルの履歴管理機能や履歴管理機能を持った情報管理システムの活用等も有用です。

  ※なお、事後的にフォレンジック技術を活用することによる情報復元の手段もあり得ますが、その前提として、事前に、上述のように履歴等の記録が取られていることが不可欠となります。

（保存しておくべき記録の内容）

- 技術情報については、当該技術が生まれるまでの実験過程等を記載したラボノートを作成・保存します。ラボノートについては、その信用力の向上の観点から、定期的に、プロジェクトに参加していない従業員による日付等の確認を行うことも考えられます。

- 営業情報、例えば顧客名簿については、顧客になるに至った経緯の記録（どの広告を見てどのようなアクセスがあったのかの記録、会員加入申込書等の原本等）、取引情報については、その作成経緯の記録として、取引経緯を記録した書面（取引伝票等の原本等）、接客マニュアルは、それらの作成に至る会議の議事録などを保存します。

（記録の信用力の向上）

- また、これらの資料について、必要に応じて、公正証書化することによって、信用力を高めることが考えられます。同様に、電子文書（例えば細かい技術仕様についての大量のデータ）については、認証タイムスタンプや電子公証を利用し、特定の日時にその秘密情報を保有していたことと、それ以降その秘密情報が改ざんされていないことを客観的に証明できるようにすることも考えられます。

５－２　他社の秘密情報の意図しない侵害の防止

○　他社の秘密情報を意図せず侵害することを防ぐためには、自社にとっての必要性の観点から、他社から受け取る秘密情報を厳選した上で、受領した他社の秘密情報は、自社情報と徹底的に分離して管理することがポイントとなります。

○　以下では、特に自社情報と他社情報の混在が生じやすいと考えられる４つの場面（（１）転職者の受入れ、（２）共同・受託研究開発、（３）取引の中での秘密情報

の授受、（４）技術情報・営業情報の売込み）を想定し、それぞれの場面で有効と考えられる対策を紹介します。以下に示す対策を行うことは、業務効率等の観点で相応のコストがかかるものの、実際に秘密情報に関して紛争となってしまった場合、損害賠償や社会的信用の低下など、対策にかかるコストをはるかに上回る損失を被る場合が多いことを認識する必要があります。

○　また、この対策を真に実効性のあるものにしていくためには、現場の従業員が自社情報と他社情報の混在のリスクを正しく理解することが必要であり、例えば社内研修等を通じて周知徹底を行うことも重要です。

○　さらに、内部監査等を通じて、自社における対策が、実際に正しく実施されているか定期的に確認を行うことも重要です。

○　なお、特に留意すべきなのは、本章５－１で述べたとおり、他社から営業秘密の開示を受けた場合に、それが不正な開示であることを知らなかったとしても、知らないことにつき「重大な過失」があるときには、その営業秘密を使用したり、更に別の他社に開示したりする行為が損害賠償請求や差止請求の対象となり得る点です。

○　加えて、平成２７年不正競争防止法改正により、営業秘密の不正使用行為を推定する規定が導入され、生産方法の営業秘密を違法に取得して、その生産方法により生産することができる製品を生産している場合には、違法に取得した営業秘密を不正使用したものと推定されることとなりました。ここでいう「違法な取得」には、不正開示であることを知らないことにつき「重大な過失」がある状態で営業秘密を取得する場合も含まれることから、特に「重大な過失」とされてしまうことのないような対応をすることが重要です。

※「重大な過失」とは、我が国企業に求められるべき取引上の注意義務に照らし、営業秘密の取得時の客観的状況から、他社の営業秘密を侵害するおそれが大きいことが容易に予期できたにもかかわらず、その疑いを払拭するための合理的努力を怠ったこと、すなわち悪意と同視し得るほどの取引上の著しい注意義務に違反したことを意味します。

※下記の対応策は、そのような「重大な過失」がないとされるために有効と考えられる取組ですが、これらの取組により、常に「重大な過失」がないとされたり、これらの取組をしていなかったからといって「重大な過失」があったとされたりするものではないことに留意が必要です。

（１）転職者の受入れ

○　他社の営業秘密の不正取得、使用等を前提とした採用・営業活動を行わないことは当然ですが、他社から転職者を受け入れる場合、その転職者が持ち込む情報の中に、転職元の秘密情報が存在する場合があるなど、会社側も意図せぬ形で他社の秘密情報を取得してしまうリスクが生じ得ます。なお、出向していた従業員が、自社に戻ってきた場合にも、以下と同様の対応策が必要となる場合があります。

○　特に、本章５－１で上述したとおり、転職者の持ち込んだ情報が他社の営業秘密であると知らなかったとしても、知らなかったことに「重大な過失」がある場合には、不正競争防止法に基づく損害賠償請求や差止請求の対象となり得るため注意が必要です。

○　なお、自社が受け入れようとしている転職者について、転職元企業の中核部署にいたことがあったかどうか、極めて高い評価を受けていたかどうかといった観点から、その転職者の立場を確認することも考えられるでしょう。転職元企業におけるキーパーソンと呼べるような人物である場合には、特に慎重に以下の対応策を講ずることが重要です。

○　以下では、①転職者の契約関係の確認、②転職者採用時における誓約書の取得等、③採用後の管理、の場面に分けて対応策を紹介します。必ずしもこのうち、いずれか１つの場面への対応で足りるということはなく、状況に応じ、必要な対策を採ることが重要となります。

①転職者の契約関係の確認

○　転職者を受け入れるに当たって、まずはその転職者が、転職元との関係で、「特定の情報を外部に持ち出してはいけない」（秘密保持義務）、「競合他社に転職してはならない」（競業避止義務）といった義務を負っていないかを確認する必要があります。

○　このように、転職者の転職元における職務内容に照らし、負っている義務の内容を明らかにしておくことで、採用後の転職者の配属を適切に決定したり、転職者が自社内において転職元の営業秘密を開示・使用していないかをより着実に確認することができ、不正競争防止法上の「重大な過失」が無いとの主張の一助となると考えられます。

○　実際には、転職元企業からの警告書面を受領し、その中に契約内容の一部が記載されて初めて転職者の負っている義務内容の一部が明らかになるようなケースもあ

ることから、まず転職者本人との間で、面接での記憶喚起等を通じた事実確認をしっかり行うことが重要です。

○ なお、仮に転職者の義務の内容を確定的に確認できなかったとしても、転職者が転職元企業との関係で秘密保持義務等を 負っている可能性はゼロではなく、そのリスクは容易に無視し得ないものである以上、必要に応じて下記②、③の取組を検討することが重要です。

具体例

- 前職の就業規則や、退職時に交わしている契約書や誓約書などを確認し、特定の情報を外部に持ち出してはいけないといった義務（秘密保持義務）や、退職後に競業に就いてはいけないといった義務（競業避止義務）等の有無や内容を面接やアンケートなど合理的な方法を通じて確認する。
- 転職者が、そのような契約書や誓約書等の写しを転職元から交付されていなかったり、その内容が「すべての情報を持ちだしてはならない」といったものであるなど、転職者が負っている義務の範囲が漠然としている場合であっても、転職者本人に対する記憶喚起やインタビュー等を通じて、できるだけ義務の範囲を特定するよう努める。
- 転職者が負う義務の有無に関わらず、②で後述するような「誓約書の取得」などの取組も着実に実施することが望ましい。なお、転職元において中核的な役割を担っていた転職者を受け入れる際には、当該技術情報の性質や当該転職者の従前の職務内容等に応じ、当該転職者が転職元企業との間で秘密保持義務や競業避止義務を負っている可能性が高いことに留意した、より慎重な対応を行うことが考えられる。
- 以上の対応を行ったことを、採用時の議事録やレポート等の書面の形で記録・保存しておく。

②転職者採用時における誓約書の取得等

○ 転職者に、転職元での秘密情報を自社内に持ち込ませないよう注意を喚起するとともに、不正競争防止法上の「重大な過失」が無いとの主張の一つの根拠とするために、転職者の採用時に書面での確約を取っておくことが有効です。

具体例

- 以下の内容（特に一点目が重要）を含む誓約書を転職者から取得する。
  ex）A 社が、B 社からの転職者 C を採用する場合における C から A 社へ差し入れる誓約書の内容。

・ 「第三者の秘密情報を含んだ媒体（データ、資料）を一切持ち出していない」
・ 「A 社の業務に従事するにあたり、B 社の情報を用いない」
・ 「第三者が保有するあらゆる秘密情報を、A 社に開示し、又は使用するように仕向ける等しない」
・ 「A 社で就業するにあたり不都合が生じる競業避止義務がない」
・ 「第三者の完成させた職務発明等を A 社名義で出願しない」
・ 「B 社の製造プロセスに関する情報を知っているが､A 社の設備の内容及び仕様等に照らして、当該情報を転用できるような状況にはない」

※この内容については、従事させる業務の具体的内容に応じて、採用後に約させることも考えられる。

➢ これらの誓約書の内容を補強する材料のひとつとして、転職者の採用の経緯や理由として、どのような能力や経験等に積極的に着目し、どのような環境でそれらを発揮することを期待しているか等を社内文書として残しておく。

③採用後の管理

○ 転職者から採用時に誓約書を取得しただけでは、必ずしも自社情報と他社情報の混在のリスクを完全に回避できるものではありません。採用後もそのようなリスクに配慮し、転職者の負う秘密保持義務等の内容を踏まえつつ、下記のような対応を行うことが考えられます。

具体例

➢ 転職者が従事する業務内容を定期的に確認する（私物のＵＳＢメモリ等の記録媒体の業務利用や持込みを禁止するといった取組も有効）。

（２）共同・受託研究開発

○ 他社（大学等の研究機関も含みます）との共同研究開発や他社から委託を受けた研究開発（受託研究開発）に際しては、自社においても同種の独自研究開発を行っている場合も多いところ、他社が独自に進めていた研究開発成果等の秘密情報の開示を受けることもあることから、独自研究開発のみを行っている場合に比べて、他社の情報と自社の情報が紛れやすい状況にあります。この場合、当該研究開発の分野に関連する情報を不用意に使用・開示してしまった場合には、他社との間の契約違反となるおそれがあり、その場合には損害賠償請求等がなされてしまう可能性があ

ります（不正の利益を得る目的又は当該他社に損害を加える目的で、営業秘密に該当する秘密情報を使用・開示する行為は不正競争防止法違反にもなり得ます）。

○　なお、共同研究先が、自社だけでなく競合他社とも並行して研究を行っている場合には、当該研究先を通じた競合他社の秘密情報との混在のリスクも生じ得るため、必要に応じて、下記の対応策とは別途、共同研究先に対しても複数の共同研究情報を混在させないように注意を促すことが考えられます。

○　以下では、共同研究開発や受託研究開発の場面において、①他社から得る情報の厳選、②秘密情報に該当する情報の明確化、③他社の秘密情報の分離管理、④自社の独自研究・開発からの他社の秘密情報の排除、の４つの視点に分けて対応策を紹介します。必ずしもこのうち、いずれか１つの場面への対応で足りるということはなく、具体的な状況に応じ、必要な対策を採ることが重要です。

○　なお、同時に、研究開発の開始前に保有していた自社の独自情報については、本章５－１で記載したような措置を講ずることにより、独自性を立証することができるようにしておくことも重要です。

①他社から得る情報の厳選

自社情報と他社情報の混在のリスクを低減するためには、他社の秘密情報を得ること自体が自社の事業遂行上のリスクを抱えることになり得るという認識の下、他社から得る秘密情報を厳選することが重要です。他社から秘密情報を得る場合には「当該情報を共同研究開発目的以外で使用しない」旨の契約が結ばれることが通常であるところ、そのような契約に合意することは、将来的に自社の独自研究開発や別の他社との共同研究開発を行う際の紛争リスクを高めることになるからです。

具体例

- 他社の情報を得る前に、将来自社において関連する独自の研究開発を行う可能性を検討する。
- その可能性を踏まえた上で、他社の情報を得ることにより、自社の事業遂行に与えるリスクを具体的に検討する。
- 他社の情報を得る場合の「当該情報を共同研究開発目的以外で使用しない」旨の契約については、「〇〇年経過後は使用できる」といった、より細かな契約条件を検討することも考えられる。

②秘密情報に該当する情報の明確化

他社から秘密情報を得ることとした場合には、共同・受託研究開発の進捗状況等に応じ、秘密情報に該当する情報をできる限り明確化することが重要です。これは、秘密情報に該当する情報が明確となっていなければ、どの情報との混在を防止すべきかという対策が立てられず、かえって自社情報と他社情報の混在のリスクを高め、無用な対策コストを支払う必要が生じるおそれがあるからです。

具体例

- 秘密保持契約を締結する際に、できる限りその対象となる情報を契約書内で明確に示す。（特に技術内容等に係る情報などは、将来の自社の独自研究開発に与える影響が大きくなることが考えられるため、社内での秘密情報の決定の場合や従業員の秘密保持義務の対象を決定する場合に比較して、より具体的・限定的に決定することが望ましい。）
  - ex）秘密保持契約書内に、相手方から開示を受け、かつ開示の際に相手方から秘密である旨の明示のあった情報についてのみ秘密情報とする旨を規定する。
  - ex）秘密保持契約書内に、相手方から受領した情報について、既に知っている情報であった場合には、その根拠とともに、その旨を申し出る義務を規定する（申し出た場合には当該情報は秘密保持の対象とならない）。
  - ex）研究開発の過程で事前に想定していた範囲や書面で合意していた範囲を超えて、事後的に口頭で秘密情報が共有される事態が考えられる場合には、それに備え、「口頭での情報開示後、一定期間内にその旨を文書化した場合に限り、秘密保持義務の対象とする」旨の規定を設ける。
- 研究開発の過程で実際にいつどのような情報を授受したかについて記録する。相手方に授受の確認のサインをもらうことも考えられる。

③他社の秘密情報の分離管理

他社から実際に得た秘密情報については、自社情報と分離して管理します。自社情報と、他社情報が混在してしまうと、他社から訴えられたときに「他社の秘密情報を使っていないこと」を立証することが極めて困難となるため、情報が混在しないための管理をしっかり行っていたことを立証できるようにしておくことが重要です。

具体例

- 他社から情報を得る窓口を設定し、その窓口以外では他社から秘密情報を受け取らないようにする（専用のメールアドレスを設定することも有効）。また、その窓口では、取得した情報の内容、取得した日時、取得

の経緯等を記録する。

- 他社の秘密情報を含む電子データは、自社情報とは別のフォルダにおいて管理する。場合によっては、そのフォルダには関係者以外がアクセスできないようにＩＤ・パスワード等でアクセス制限を行い、アクセスログを記録する。
- 化合物や試作品のように物それ自体が秘密情報に該当する場合は、特別のキャビネットや倉庫等において、自社情報と分離して保管する（施錠した上で、その鍵の貸出し記録や、その物の持出し記録を作成することも考えられる）。
- 自社における共同・受託研究開発の関係者（他社の営業秘密に接する必要のある従業員等）を特定し（必要に応じてリスト化して特定の手続でのみ当該リストを変更可能なものとすることも考えられる）、その全員から「当該情報を共同・受託研究開発の関係者以外に開示しない」、「当該情報を共同・受託研究開発目的以外で使用しない」旨の誓約書を取得する。
- 共同研究開発終了後に、確認書を取得し、誓約が遵守されたことを改めて確認する。

④自社の独自研究・開発からの他社の秘密情報の排除

自社において独自に、他社の共同研究・開発と内容的に類似する研究・開発等を実施する場合には、当該他社から秘密情報を取得ないし使用したとして訴えられるリスクを低減するため、自社独自の研究・開発に使用する情報の中に、当該他社から得た秘密情報が紛れ込んでしまうことを防止する措置を講ずる必要があります。

具体例

- 自社の独自研究開発の関係者を特定し、その全員から「当該他社の営業秘密に接触しない」又はその者が共同・受託研究開発にも携わる必要がある場合には「当該他社の営業秘密を自社の研究開発現場に持ち込まない」旨の誓約書を取得する。
- 自社の独自研究開発を開始するときに、その研究開発に使用する情報の中に、共同・受託研究開発に関する情報が含まれていないかを厳重に確認する。自社の独自研究開発に途中から参加する従業員がいる場合には、その従業員のＰＣ等もチェックする。また、共同・委託研究開発には専用の初期化されたＰＣを別途貸与することも考えられる。
- 上述のように情報を分離することに加えて、自社開発を行う者の中に、共同研究開発に携わる者を含めない（自社開発と共同研究開発の担当者を分ける）ことが望ましいが、人員との関係で難しい場合には、①自社

開発で使用する情報を明確化する、②自社の研究開発現場と共同研究開発現場を物理的に別部屋とする、③それぞれの開発経緯を詳細に記録する等、更に厳格に情報を分離する対策を実施することが考えられる。

（３）取引の中での秘密情報の授受

○ 日常的に行っている取引の中で、取引先から秘密情報を取得することは少なくありません。例えば、委託契約や請負契約等において、相手方から秘密情報の開示を受けることがあります。

○ このうち、特に留意すべき点としては、①委託者や注文者からではなく、受託者や請負人、下請企業等から秘密情報が開示される場面も想定されますが、これらの場面では委託者や注文者から秘密情報が開示される場面に比して、その情報の適切な管理の必要性について気づきにくい可能性があります。

○ 特に、②商品サンプル等それ自体が秘密情報である物の受領の場面については、発注者である自社が、不正な利益を得たり、取引先に損害を加えたりする意図で当該商品サンプル等を使用・開示しないことは当然のことです（その場合には不正競争防止法上の民事・刑事責任（※）を問われてしまいます）が、そのような意図がないとしても、秘密表示が付された書類等に比べて、取引先の秘密情報を受領しているという意識が低くなることもあり得ます。

※平成２７年不正競争防止法改正により、営業秘密侵害罪が非親告罪化となったことにより、当該取引先の意思によらず、刑事訴追される可能性もあることに留意が必要です。

○ したがって、これらの場面においては提供された秘密情報と自社情報との間で混同のリスクが高まる可能性があり（このケースについても、（２）共同・受託研究開発のケースと同様、契約違反に基づく損害賠償請求や差止請求がなされることが考えられる）、意識的に対応策を講ずることが考えられます。

具体例

- 社内研修などを通じて、日常的な取引における秘密情報の授受の可能性や、商品サンプルや試作品等は、それ自体が他社の秘密情報に該当し得る旨を従業員に対して周知する。
- 秘密情報の開示や商品サンプル・試作品等の受領が、口頭やメールでのやり取りに留まって行われた場合であっても、秘密保持契約が成立していたとして提訴されるリスクが存在することから、取引先の秘密情報の内容や、使用目的の制限、秘密保持の期間などについて、書面により確認をすることが望ましい。

- 当該商品サンプルや試作品等を含む秘密情報を取り扱う自社従業員を限定した上で、「当該取引以外の目的で当該情報を使用・開示しない」といった誓約書を取得したり、特別のキャビネットや倉庫等において、自社情報と分離して保管したりするなど、（２）共同・受託研究開発のケースと同様の取組が有効である。

（４）技術情報・営業情報の売込み

○ 外部の研究者等が独自研究したものとして技術情報を売込みに来たり、何者かが顧客名簿等の営業情報を売込みに来たりした場合、実はその売り込まれた情報が他社の公開前特許等の秘密情報であったり、盗まれた顧客名簿であることもあり得ることから、当該情報と自社情報の混同のリスクが生じます。

○ 特に、上述したとおり、売り込まれた情報が他社の営業秘密に該当する場合には、その事実について知らなかったとしても、知らなかったことに「重大な過失」がある場合には、不正競争防止法に基づく損害賠償請求や差止請求の対象となり得るため注意が必要です。

具体例

- 売り込まれた情報の出所や、どのようにしてその情報を取得したのか等を売り込みに来た者に確認し、「当該情報は○○（出所）から正当に取得したものである」旨の誓約書等を取得することが望ましい。また、情報を売り込みに来た者から確認した事実について、可能な範囲で関係者に事実関係を聴取することなども望まれます。
- その確認した内容等を踏まえてなお、他社の秘密情報の不正な売込みである疑いが相当程度残る場合には、その売込みには応じないことが重要です。

５－３　営業秘密侵害品に係る紛争の未然防止

○ 平成２７年不正競争防止法改正により、営業秘密を不正に使用することによって生じた物（営業秘密侵害品）の譲渡・輸出入等の行為が、民事措置（損害賠償請求・差止請求）の対象に含まれることとなりました。これは、営業秘密を不正使用した張本人（例えば、他社の営業秘密にあたる技術情報を不正に入手し、それを用いて製品を製造したメーカー）でなくとも、それが営業秘密侵害品であることを知って、又は知らないことについて「重大な過失」がある状態で、その営業秘密侵害品を譲り受けた者が、その営業秘密侵害品を譲渡・輸出入等する行為（例えば、営業秘密

を侵害して作った製品であることを知っている小売業者による販売行為や商社による輸出行為）も民事措置の対象となります。

○ また、これらの行為のうち、営業秘密侵害品であることについて、それを譲り受けたときに認識した上で、意図的に譲渡・輸出入等を行った場合には、民事措置のみならず、刑事措置の対象にもなり得ます。

○ よって、他社との間で製品の売買等の取引をする場合には、そのような「重大な過失」があると判断されてしまうことのないように特に注意を払う必要があります。

○ ただし、この「重大な過失」とは我が国企業に求められるべき取引上の注意義務に照らし、営業秘密の取得時の客観的状況から、他社の営業秘密を侵害するおそれが大きいことが容易に予期できたにもかかわらず、その疑いを払拭するための合理的努力を怠ったこと、つまり悪意と同視し得るほどの取引上の著しい注意義務に違反したことを意味し、通常の企業活動を行っている場合にはこの「重大な過失」があるとされることは極めて限定的であることが想定されます。すなわち、実際に、自社の取引するすべての製品に対して、取引の都度、営業秘密侵害品であるか否かの確認を行うことは現実的ではないことから、基本的には、他社から「営業秘密侵害品である」との警告書を受領したり、取引相手が営業秘密侵害を行っている疑いがあるとの情報が業界内で広がっているといった「疑わしい状況」が生じている場合に、相当の注意を払ったということが証明できる程度の対策を行うことが肝要です。

具体例

- 自社が取引する製品について、「営業秘密侵害品である」との警告書を他社から受けた場合、まずはその書面が、侵害された営業秘密の内容や、どのような経緯で侵害がなされたか、いかなる理由で侵害の事実を確信したか、といった具体的な内容を伴うものであるか否かを確認する。
- 具体的な内容を伴う警告書である場合には、その内容について取引先などの関係者にその真偽を確認する。それを踏まえて、取引する製品が営業秘密侵害品であるとの疑いが相当程度残る場合には、それ以降の製品の取引は一旦中止することが望ましい。一方、取引を継続する場合には、取引先などの関係者から「営業秘密を侵害して生産したものではない」旨の誓約書を取得する。
- 例えば、「営業秘密の侵害事案について報道がなされた」、「自社の販売する商品と同じメーカーが製造する同一ラインナップの商品について差止請求訴訟が認容された」、「取引相手が営業秘密侵害を行っている疑いがあるとの情報が業界内で広がっている」といった「疑わしい状況」

が生じた場合にも、上記と同様の確認を行う。

※なお、警告書が電子メールで送付されることもあり得るところ、警告書を装った標的型メール等には十分に留意して対処することが必要。

第６章　漏えい事案への対応

- 企業が情報管理をどれだけ徹底したとしても、昨今のサイバー攻撃をはじめとする情報漏えい手口の高度化等を踏まえると、情報漏えいを完全に防ぎ切ることは困難であり、万が一情報漏えいが起こった場合に迅速に対応できるよう備えておくことが重要です。
- 対策に当たっては、（１）情報漏えいの疑いを確実・迅速に確認できるようにすること、（２）情報漏えいが起こってしまったと思われる場合に、その被害を最小限に抑え、また原因究明・責任追及に係る証拠を保全するための応急措置を迅速に実施すること、（３）被害回復（損害賠償・差止）と将来的な再発抑止のための徹底的な責任追及を実施すること、の３点がポイントとなります。
- なお、漏えい時に適切な対応をするためには、第２章及び第３章の漏えい防止対策を講ずるとともに、第４章の社内体制を整え、また万が一紛争に発展してしまった場合を見据えた第５章に記載する事前の備えをしていることなど、漏えい後の対応だけではなく、日頃からの備えをしておくことが重要となります。

６－１　漏えいの兆候の把握及び疑いの確認方法

○　企業の重要な情報が漏えいした場合、多くの場合、その被害は時間の経過とともに拡大します。速やかに情報漏えいに対処し、その被害を最小限に抑えるためには、事前に情報漏えいに繋がり得る兆候を把握（以下（１））し、その兆候を確認すること等を通じて、漏えいの疑いを確認し（以下（２））、速やかに対処することができる体制・社内ルールを構築していることが必要です（第４章も参照）。これらの取組は、第３章で示した「視認性の確保」等にも資する場合が多いことから、同時に情報漏えいを未然に防止することにも繋がると考えられます。

（１）漏えいの兆候の把握

○　ここでは、漏えいの主体に応じて、情報漏えいに繋がり得る兆候と考えられる具体例を記載します。具体的には、①従業員等、②退職者等、③取引先、④外部者ごとに記載をしています（それぞれの定義は第３章に記載）。

○　下記のような兆候を適切に発見するためには、日頃から自社の通常の業務状況とは何かを把握しておくことが重要です。例えば、下記①に記載の「業務量に比べて異様に長い残業時間」といっても、各企業・各部署の状況に応じて、どの程度の時間の残業が「異様」と言えるのかは異なります。

○　具体的には、自社の従業員の勤務状況等について、タイムカードによる業務時間の把握や、部署内での報告、定期的な面談による業務量の確認等を通じて、どのような状態が「異様」と言えるのかを意識しておかないと、従業員の残業が情報漏えいに繋がり得る兆候に当たるのかどうかの判断が難しいでしょう。

①従業員等の兆候

従業員等の情報漏えいの兆候としては、例えば以下のものが考えられます。

- （業務上の必要性の有無に関わらず）秘密情報を保管しているサーバーや記録媒体へのアクセス回数の大幅な増加
- 業務上必要性のないアクセス行為
  ex）担当業務外の情報が保存されたサーバーやフォルダへの不必要なアクセス
  ex）不必要な秘密情報の大量ダウンロード
  ex）私物の記録媒体等の不必要な持込みや使用
- 業務量に比べて異様に長い残業時間や不必要な休日出勤（残業中・休日中に情報漏えいの準備等を行う従業者が多いことから兆候となり得る）
- 業務量としては余裕がある中での休暇取得の拒否（休暇中のＰＣチェック等による発覚を恐れるため兆候となり得る）
- 経済的、社会的に極めて不審な言動
  ex）給与に不満を持っているにも関わらず急激な浪費をし始めた
  ex）頻繁に特定の競合他社と接触している

②退職者等の兆候

退職者等の漏えいの兆候としては、例えば以下のものが考えられます。特に、中核的な業務に携わっていた者など、キーパーソンといえる元従業員についてはその退職前後を通じた動き（転職先企業の業務内容を含む）の把握が重要となります。

- 退職前の社内トラブルの存在
- 在職時の他社との関係
  ex）競合他社から転職の勧誘を受けていた
- 同僚内の会話やＯＢ会等で話題になっている、元従業員の不審な言動
  ex）競合他社に転職して、前職と同じ分野の研究開発を実施しているとの取引先からの情報提供
- 退職者の転職先企業が製造・販売を開始した商品の品質や機能が、特に転職後、自社商品と同水準となった

③取引先の兆候

取引先の漏えいの兆候としては、例えば以下のものが考えられます。

- 取引先からの突然の取引の打ち切り
  ex）自社しか製造できないはずの特別な部品について、発注元からの部品発注が途絶えた
- インターネット上での取引先に関する噂
  ex）インターネット掲示板、SNS 等において、自社製品との類似品が取り沙汰されている
- 取引先からの、取引内容との関係では必ずしも必要でないはずの業務資料のリクエスト
- 自社の秘密情報と関連する取引先企業の商品の品質の急激な向上
- 自社の秘密情報と関連する分野での取引先の顧客・シェアの急拡大

④外部者の兆候

外部者の漏えいの兆候としては、例えば以下のものが考えられます。

なお、不正アクセスなどのサイバー攻撃については、その兆候を把握しにくく、実際に情報漏えいの被害が発覚したときが最初の兆候となる場合も多いため、その兆候をいち早く把握するための日常的な管理体制の構築が特に重要と考えられます。

- 自社における事件の発生
  ex）社員証・パスワードなどの流出事件の発生
  ※流出の態様としては、典型的には盗難行為であるが、巧みな話術による聞き出し、盗み聞き・盗み見等を通じた流出があり得ることにも留意
  ex）社員の机上の物など、オフィスにおける盗難事件の発生
- 自社会議室における偵察機器（盗聴器など）の発見
- 競合他社等での秘密情報漏えい、不法侵入等の事案発生（類似の技術を持つ自社の情報についても狙われやすいと考えられるため兆候となり得る）
- ウイルス対策ソフト、セキュリティ対策機器による警報
- 自社の秘密情報それ自体ではないが、それと不可分一体のはずの情報が漏えいしていること
- 電話、メール等を受信した関係者からの通報
  ex）自社の顧客名簿に記載された者が、競合他社から営業の電話を受けたが、その競合他社に連絡先を教えた覚えがないため、不審に思ってその旨連絡をしてきた

ex）他所における侵害を調査していたセキュリティ調査機関が、侵害されたサーバーにおいて自社の情報を発見したと連絡してきた

（２）漏えいの疑いの確認

○　上記（１）により情報漏えいに繋がり得る兆候を把握した場合には、その兆候を放っておくことなく、情報漏えいが発生した疑いが高いものとして初動対応を開始する必要がないかを確認する必要があります。いかなる者による情報漏えいの兆候であったかにより、有効な確認方法が異なることから、兆候が生じた者に応じた確認方法を取ることが必要であると考えられます。したがって、以下では上記（１）の分類に応じて、その漏えいの疑いを確認するための対応策として考えられる具体例取組を示します。

○　なお、以下の取組を実施するにあたっては、兆候のあった直近の時点だけではなく、ある程度過去に遡って、事実や状況の確認を行う必要がある場合があるという点に留意してください。

①従業員等による漏えいの疑いの確認

従業員等による漏えいの疑いを確認するための取組としては、例えば以下のものが考えられます。なお、メールのモニタリングや社内ＰＣのログ確認については、そのような措置を行うことがあり得ること等を事前に就業規則で定めておくなどすると、手続的な問題は起こりにくくなるでしょう。

具体例

- 文書管理台帳等による情報保有状況の確認
  ex）紙媒体の資料やＵＳＢメモリ等の記録媒体のリスト管理により、漏えいの兆候のある者による重要情報の不正な持出しがないかを精査する
- 漏えいの兆候のある者の社内ＰＣについて、ＵＳＢメモリ等の記録媒体の接続ログの確認
- 漏えいの兆候のある者の社内ＰＣのログ等の保存・確認や、メール送信、インターネット利用履歴のモニタリング（場合によっては社内ＰＣを没収して調べることも考えられる）
  ex）業務メール、インターネット上でのメール、外部ストレージ（クラウドサービス等）へのアップロードなどを通じた不正なデータ送信の確認
  ex）漏えいの兆候のある者の社内サーバー、フォルダ、電子データへの

アクセスに関するログの詳細な確認

※一定以上の量のダウンロードがあった場合に自動でアラートの鳴るシステムを導入することなどは、速やかに漏えいの疑いの確認に取りかかることを可能とするという観点から有効と考えられます。

- 秘密情報を含む幹部宛のメールが、漏えいの兆候のある者の個人アドレスへと自動転送されるような不正な設定がなされていないか確認
- 社内規程等に基づく監査の実施

②退職者等による漏えいの疑いの確認

退職者等に関して、退職予定者等による漏えいの疑いの確認については、上記①と同様の取組を行うことが考えられますが、退職後に特有の確認としては、退職者の転職先把握が特に重要です。仮に競合他社への転職の事実が確認できた場合には、速やかに本章６－２以降に記載の初動対応の開始を検討することが考えられます。

具体的な取組としては、例えば以下のものが考えられます。

具体例

- 漏えいの兆候のある退職者等の転職先企業及びその業務内容について、元同僚らへの事情聴取、ＯＢ会等、内部通報窓口、新聞紙面上の会社人事情報といった様々なルートでの情報収集
- 漏えいの兆候のある退職者の退職前後での資料の大幅な減少の有無の確認
- 社内資料のリスト管理等による、漏えいの兆候のある退職者等の未返却物の確認
- 漏えいの兆候のある退職者等の退職前一定期間のダウンロードデータの内容チェック
- 漏えいの兆候のある退職者等の退職前一定期間のメール等の通信記録のモニタリング

③取引先による漏えいの疑いの確認

取引先による漏えいには、第３章で記載したとおり、大別して、

（ｉ）取引先自体が漏えいを行う場合

（ii）取引先の従業員、退職者、再委託者や外部者等を通じて漏えいする場合の２通りの場合があり得ます。

（ii）の場合は委託先等の社内において、本項①、②、④の取組を実施することを契約等で確保するといった取組が考えられます。以下では、（ｉ）の場合について有効と考えられる取組の例を掲載します。

具体例

- 漏えいの兆候のある取引先等の製造・販売している商品のチェック
  ex）取引先が製造・販売する商品の品質や機能が、兆候を把握した時期の前後において、自社商品と同水準となった
- （顧客名簿等に意図的に入れた）トラップ情報の使用の確認
  ex）顧客情報の中に意図的に自社や協力会社の住所を利用したダミー情報を入れておいたところ、そのダミーの宛先に郵送物等が届いた場合
- 漏えいの兆候のある取引先に自社のサーバーを使わせていた場合には、そのアクセスやダウンロードの履歴をチェック

④外部者による漏えいの疑いの確認

外部者については、例えば以下の取組を行うことが考えられます。

具体例

- 競合製品・類似商品のチェック
  ex）他社が製造・販売する商品の品質や機能が、兆候を把握した時期の前後において、自社商品と同水準となった
- （顧客名簿等に意図的に入れた）トラップ情報の使用の確認
  ex）顧客情報の中に意図的に自社や協力会社の住所を利用したダミー情報を入れておいたところ、そのダミーの宛先に郵送物等が届いた場合
- パスワードの流出した端末に対する不正アクセスの有無の確認
- 自社内への不法侵入等がないかどうか、監視カメラの記録映像を確認
- 社内資料のリスト管理による、書類や記録媒体等の持出しの有無の確認
- ウイルス対策ソフト、セキュリティ対策機器等を用いて、不正アクセスやサイバー攻撃の有無を確認

６－２　初動対応

○　情報漏えいの疑いを確認し、初動対応の必要があると判断した場合、被害の拡大防止や企業イメージの保護、迅速かつ適切な法的措置のために、適切な初動をとることが重要です。

○　スムーズな対応を行うためには、日頃から連絡体制や対処要領を準備しておくことが考えられます[22]。

具体例

- 有事における組織体制や、レポートラインの確保につき、事前に社内マニュアル等で明文化しておく（第４章●ページも参照）。
- 平時から、情報漏えいを見据えた取組を実施する。
  ex）情報漏えいが実際に起こったと仮定して、社内での対処（部門間での情報共有、対策チームの招集、初動対応の手順、報道対応等）を訓練（机上訓練・実地訓練）する
  ex）実際に社内システムを攻撃し、侵入できないという事実によってその安全性を確認する（ペネトレーションテストの実施）

（１）社内調査・状況の正確な把握・原因究明

情報漏えいの状況を正確に把握し、将来的な再発防止に資するため、まずは下記の観点から、現時点で把握できていること、できていないことについて書面等を用いて社内で明らかにします。

いつ：いつ漏れたか。一度だけか。数回に分けて漏れたか。漏えいを把握するまでの時系列は。

だれが：誰が漏らしたか。社員か、委託先か。その者はどのような権限を持っていたか。外部者の場合、自社とどのような関わりがある者か。

なにを：漏えいした情報の内容は何か。どのくらいの量の情報が漏れたか。どのような形で保存されていた情報か。

どのように：どのような方法・原因で漏えいしたか。ネットワークを通じたものか。どのようにセキュリティが破られたか。

（２）被害の検証

上記（１）で明らかになった事実を元に、自社、取引先、消費者等に対して、どのような損失（間接的な損失や信用の低下を含む）が予測されるか、最悪の事態を想

22　独立行政法人情報処理推進機構「組織における内部不正防止ガイドライン」p.59～p.60、「情報漏えい発生時の対応ポイント集」も参照。コンピュータセキュリティのインシデント対応体制については、日本シーサート協議会の HP「CSIRT 構築に役立つ参考ドキュメント類」も参照。http://www.nca.gr.jp/activity/build-wg-document.html

定して検証を行います。この検証を通じて、更に対応を進める必要があると判断される場合には、以下のような対応を進めていきます。

（３）初動対応の観点

以下に示す取組が主なものとして考えられますが、情報は素早く拡散してしまうことや秘密情報の漏えいによる損失は回復が困難であること等に鑑みると、全体として、迅速な対処をすることが肝要です。特に、コンピュータウイルス等による被害の場面では、表面的に発覚したウイルス被害にのみ対処するのではなく、探知が困難な形でより深刻なウイルスが埋め込まれている場合もあるため、技術的専門家[23]に相談することが望まれます。

〇更なる拡散の防止

具体例

- 自社情報端末のネットワークからの遮断（主にサイバー攻撃による漏えいの場合）
- 漏えいしたと疑われる者等に対する警告書の発出
- ＨＰ等に漏えいした情報が開示された場合、当該情報のインターネット上からの削除要請

〇法律に基づく手続

具体例

- 個人情報の場合、個人情報保護法に基づき、業種に応じた主務官庁に対する報告等の対応が必要
- 監督官庁等との間で、各種業法などの法令上、要求されている手続を実施

〇企業イメージを含む損失の最小化

具体例

- 把握している事実につき、速やかな対外公表（事実経緯、漏えいした情報の内容、漏えいの原因、再犯防止策、問い合わせ窓口等について）の実施
- 顧客名簿流出時の被害者対応・マスコミ対応
  ex）被害者が特定できている場合等には被害者への事実の連絡及び謝罪。

[23] http://www.ipa.go.jp/security/anshin/

ex）被害者が不特定多数であって今後の被害拡大の可能性が高い場合には、個別の謝罪に先だって公表することも考えられる。

- 刑事事件に発展する可能性のある場合には、証拠隠滅や逃走を防止するためにも、警察に事実公表のタイミングや内容について早期に相談することが有効な場合もある。
- 共同研究の成果の漏えいなど、他社の情報が併せて流出しているおそれのある場合には、当該他社に対して対応を相談することが望ましい。

（４）初動対応の体制

○ 以上の初動対応については、様々な部署が関係部署として想定されるところ、関係部署が綿密に連携して、適切かつ迅速に対処する必要があります。比較的小規模な企業の場合には、経営層が全体を統括しながら対応を進めていくことが考えられます。

○ 一方で、企業規模によっては、役員をヘッドとした組織（対策チーム）を設置することが考えられます。この対策チームには、必要に応じて外部の専門家を含めることも考えられます。ただし、対策チームの人員は、社内での情報拡散を防止する観点から、必要最小限の人数で構成し、かつ扱っている内容については秘密保持を徹底することが考えられます。

○ 場合によっては、第４章で紹介した「秘密情報管理委員会」の枠組みを利用して、対策チームの機能を行わせることも考えられます。ただし、この場合にも、「秘密情報管理委員会」の構成員のうち、必要最小限の範囲で情報を共有することが望まれます。

６－３　責任追及

○ 自社における被害回復と将来的な漏えいの抑止のため、徹底的な責任追及を実施します。

○ その前提として、責任追及の確実性と証拠収集の効率性を見据えて、どの情報を責任追及に係る「営業秘密」とするのかを明確にするという点にも留意します。

○　なお、刑事と民事でいずれの措置（又は双方の措置）を採るかについては、相互に関係はなく、警察や弁護士等の専門家に相談しつつ、具体的事情に応じて臨機応変に決定すべきと考えられます。

（１）刑事的措置

○　刑事責任の追及には、警察の関与が不可欠であるため、まず近場の都道府県警察本部の担当課に相談に行くことが考えられます。その際には、会社の方針や社内調査の結果等を説明できる担当者が相談に行くことが好ましいと考えられます。

○　場合によっては、必要書類が整うのを待たずして、上記６－２（３）の初動対応の一環で早急に警察へ相談するという選択肢もあり得ます（いかなる資料を、どのように確保すれば良いかといった証拠保全等について、警察から指導を受けられる場合もあるため）。ただし、この段階では情報の漏えいに関する資料（持ち出したことを示す証拠等）が不足していることから捜査が開始できない場合もあることにも留意が必要です。

○　また、刑事事件記録の民事裁判における活用についても、弁護士に早めに相談することが考えられます。

○　捜査開始後は、多数の関係者からの事情聴取、社内の実況見分等について、警察と連携・協力していくことが重要です。

（２）民事的措置

○　民事責任の追及の手段としては、当事者間の交渉による解決の他、民事裁判を提起して損害賠償請求権の行使等を行うことが考えられますが、それに先立って、民事保全手続で裁判前に権利の確保を求めることができます。

○　また、ＡＤＲ（裁判外紛争解決手続）の活用により、非公開の手続での柔軟な紛争解決手段を検討することも考えられます。紛争の存在自体をオープンにすることに抵抗があり、かつ、任意の交渉では話し合いがまとまらないときなどに利用することが考えられます。

○　具体的にどのようなタイミングで、いかなる手段によって民事責任を追及するべきかはケースバイケースの判断であり、適切な損失回復のためにも、弁護士等の専門家と十分協議の上、決定することが望まれます。

＜裁判外の交渉＞

【内容】

- 当事者間で行う、紛争解決のための話し合い全般をいう。

【特色】

- 法律の要件やルールにとらわれずに、当事者の任意で柔軟な解決手法を採ることが可能。

【留意点】

- 裁判所等の第三者の関与がないため、話がまとまらないおそれがある。

＜民事保全手続＞

【内容】

- 裁判を起こす前に、将来の権利を保護するため、仮の権利状態を確保しておくための手続。
- 営業秘密侵害が疑われるケースでは、営業秘密の開示・使用の仮の差止めや、競合他社への就職の仮の差止め等が考えられる。
- 裁判官との面接（当事者双方が出席する審尋期日を含む）を数回程度行い、差止め等の可否を決定する。
- あくまで仮の手続であり、その後に正式な民事裁判をし、勝訴するまでの間のみ差止めを目指すもの。

【特色】

- 手続は非公開。
- 裁判手続等に比べて迅速な対応が可能。
- 手続費用は低廉（申立人、被申立人一人ずつの場合、一件 2000 円）。ただし、仮の差止めが認められるためには、本体の訴訟で判断が覆った場合に備えた担保金（担保の有無や額は裁判所が決定）が必要な場合あり。

【留意点】

- 差止め等を認めてもらうためには、実務上は民事裁判手続と同程度の証拠が必要である（民事保全手続は仮の差止めを求めるものにせよ、営業秘密の使用等を一定期間止められるという効果は、事実上民事裁判に勝訴したときと類似するため）。

＜民事裁判手続＞

【内容】

- 営業秘密の使用の差止請求、営業秘密の漏えいによる損害賠償請求等を求める裁判手続。
- 例えば、自社従業員が競合他社へ転職した際に営業秘密を漏えいした事

例では、その営業秘密の使用の差止め、その営業秘密の廃棄、その営業秘密の使用により生じた生産物の廃棄などを請求することが可能。同時に、自社従業員が競合他社へ転職した事例では、既に当該従業員に対して退職金の支給を行っていた場合、当該退職金の返還を求める裁判などが考えられる。

【特色】

- 手続は公開。
- 手続費用は民事保全手続に比べて高額であり、その具体的金額は請求内容（損害賠償請求額）に応じて変動する。

【留意点】

- 裁判手続はその終結までの間に年単位での期間を要する場合も多い。

＜ＡＤＲ（裁判外紛争解決手続）＞

【内容】

- 裁判によらず公正中立な第三者が当事者間に入り、話し合いを通じて解決を図る手続。仲裁（中立な第三者による一定の判断が下されるもの）、調停・あっせん（いずれも中立な第三者の仲介による解決合意）など様々なものが存在。

【特色】

- 手続は非公開であるため、係争の事実等が明るみに出ないで済む。
- ニーズに応じて仲裁、調停、あっせんを選択できるなど、裁判外紛争解決手続の利用の促進に関する法律の枠内で、比較的柔軟な対応が可能。

【留意点】

- 相手方がＡＤＲ手続の開始に同意しないと、手続を行うことができない。

（３）社内処分

以上の刑事責任や民事責任の追及の他、従業員による漏えいに対しては、社内での処分（懲戒免職、降格等）を行うことが考えられます。そのためには、日頃から、漏えい事案に適正に対処できるような社内規程になっているか、確認しておくことも重要です。

※ただし、従業員に対し過度な萎縮を及ばさないように配慮が必要です。

６－４　証拠の保全・収集

○　本章６－１から６－３までに記載した、漏えいの兆候の把握及び疑いの確認、初動対応、責任追及の全ての過程を通じて、各過程で必要となる範囲で、段階的に、かつ、着実に、漏えいの事実を裏付ける証拠を積み上げることが重要です。

○　その際に重要なのは、証拠の入手・生成方法を明らかにしておくことによって、証拠の保全・収集の正当性（改ざん等をしていないこと）を担保することや、事後的に共犯者が発覚した場合等に備えて得た情報を一定期間保存しておくことによって、保全・収集した証拠をきちんと利活用することができるようにしておくことです。

○　ここでは、責任追及のための準備段階（漏えいの兆候の把握、疑いの確認、初動対応）（以下（１））と、実際に責任追及を行っていく段階（以下（２））とに分けて、証拠保全・証拠収集に関する具体的取組として考えられるものを紹介します。

（１）証拠の保全

○　証拠の中には、特に電子情報など、時間の経過とともに失われやすく、時宜を逃すと証拠を確保することができなくなってしまうものが存在するため、そのような情報については、迅速な証拠の保全が求められます。

○　まず、早期に社内のネットワークやセキュリティの担当者と連携することが重要になります。

○　ただし、専門家を通さず自社だけでやみくもに保全を行おうとすると、場合によっては情報が壊れてしまったり、改ざんを疑われて事後的に証拠価値が失われる場合もあり得ますので留意が必要です。警察に即座に通報する、専門業者（フォレンジック等）を活用するといった、専門的な知見を持った者と適宜連携することが安全な場合が多いと考えられます。

○　また、まだ漏えいの証拠が十分に確保できておらず、漠然と漏えいが疑われるに留まる段階で、当該漏えい行為をしたと考えられる従業員に接触する（不用意に事情聴取を行う）など拙速な対応をすることは、かえって証拠隠滅を助長するおそれなどがあるため避けるべきです。自社従業員からの漏えいが疑われる場合には、その漏えいの疑いに関する事情について対策チーム等の関係者限りとするなど、慎重に対応して証拠の隠滅・散逸等を防ぐことが重要です。実際にいかなる対応をすべきかは、警察や弁護士等と相談することが望まれます。

○　この他、民事訴訟法に基づく証拠保全手続が有効なケース（漏えいの疑われる者の自宅に所在する書類に対する証拠保全手続等）も考えられる。

○　以下は、上記６－１（２）における漏えいの疑いの確認のための具体的方策に加えて、特に証拠の保全の観点から重要と考えられる取組となります。

具体例
- 社内ネットワークのアクセスログや、監視カメラ等の記録を保存
- 漏えいが疑われる従業員のＰＣ等のバックアップ・通信記録保存・解析
- 漏えいの疑われる者から携帯電話やＰＣ等の通信記録の開示を受けることに成功した場合は、写真撮影等による証拠化

（２）証拠の収集

○　実際に責任追及を行っていく段階に用いる証拠を収集するにあたっては、特に営業秘密に該当すると思われる情報に関して、不正競争防止法に違反する事実を証明することを意識することが重要です。

○　すなわち、まず、漏えいされた秘密情報が同法で定義される営業秘密に該当するための要件として、①秘密管理性、②有用性、③非公知性が挙げられます（同法第２条第６項）。また、それに加え、営業秘密侵害による刑事責任を問うためには同法第２１条第１項、民事責任を問うためには同法第２条第１項第４号から第１０号までの要件等をそれぞれ満たす必要があります。

○　したがって、以下では、これらの条文に掲げられた行為があったことの証拠となり得るものとして、考えられる具体的な資料の例を掲載します。

○　いずれにせよ、証拠を収集するにあたっては、警察や弁護士等の専門家に相談した上で適切かつ迅速に責任追及の準備を進めることが望まれます。

※なお、秘密情報の侵害行為が、不正競争防止法に違反すると同時に、不正アクセス禁止法等の他の法令に抵触するケースもあり得る。

＜営業秘密の要件該当性（特に秘密管理性）の証明に有効な資料例＞
- 情報の管理水準が分かる資料（就業規則、情報管理規程、管理状況に関する社内文書等）
- 漏えいが疑われる者と自社との間で交わされた秘密保持誓約書

- 情報の取扱いに関する社内研修等の実施状況に関する社内記録
- 特定の情報に対するマル秘マークの付記、アクセス制限、施錠等の情報の管理状況に関する社内記録
- 漏えいが疑われる者が、漏えいに係る情報が秘密であることを認識できたことを裏付ける陳述書（社内における実際の管理状況や、口頭での情報管理に係る注意喚起の状況等）

＜不正競争防止法違反の要件該当性の判断に有効な資料例＞

- 漏えいが疑われる者の立場（アクセス権の保有者であったか、会議等で資料を配付された者であったか、外部者であるか）に関する社内記録
- 漏えいが疑われる者が自社従業員である場合には、どのような秘密保持に係る任務を負っていたかが分かる就業規則、秘密保持誓約書
- 漏えいが疑われる者が委託先である場合、委任契約書、秘密保持契約書
- 情報持ち出しの具体的行為態様が分かるアクセスログ、メールログ、入退室記録、複製のログ
- 漏えいが疑われる者の行為目的が窺える他社とのメールや金銭のやりとりに関する書面
- 情報漏えいの発覚の経緯を、社内調査等に基づき時系列的にまとめた文書