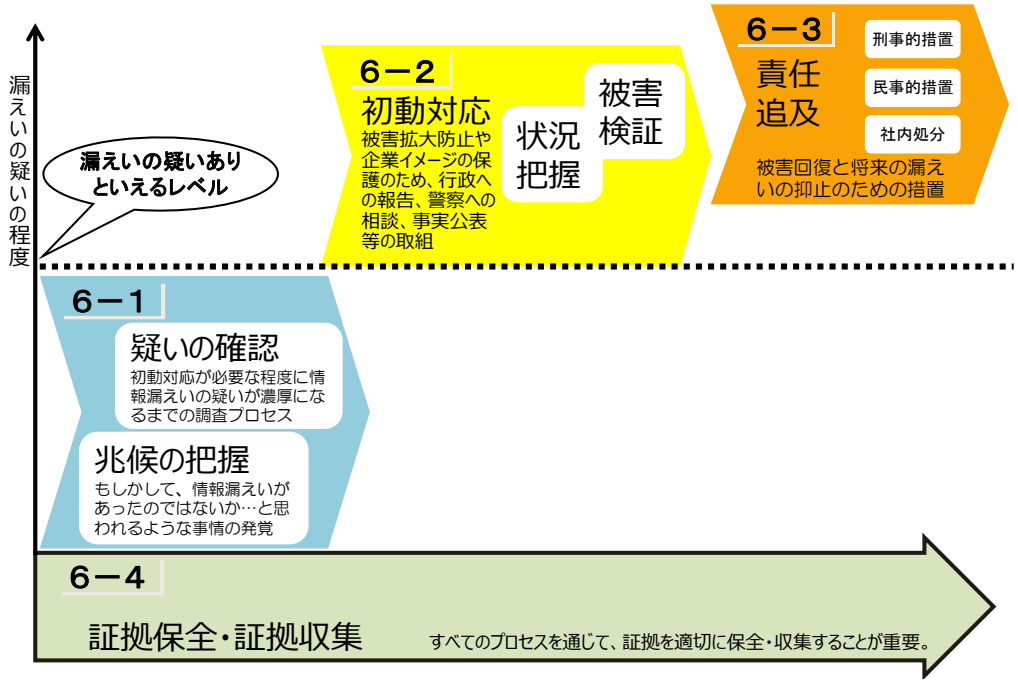
第６章　漏えい事案への対応

- 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、その損失を最小限に抑え、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）損失回復（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。

図表６（１）本章における各項目の関係



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つな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）。これらの取組みは、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つな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、情報漏えいにつな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）。

○　以下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や取引の実態を把握しておくことが重要です。例えば、以下①に記載の「業務量に比べて異様に長い残業時間」や以下③に記載の「取引先からの異様に詳細な情報照会」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、取引の実態に照らしてどの程度の情報開示が通常と言えるのかは異なります。

○　具体的には、例えば、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つな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、ＨＰ等において、自社の非公開情報や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や通常の取引に比べて異様に詳細な情報照会
- 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）
- ウィルス対策ソフト、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

○　前述（１）により情報漏えいにつな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、以下では前述（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みを示します。

○　なお、以下の取組み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みとしては、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[43]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。
- 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

[43] 参考資料２の「第１　秘密情報管理に関する就業規則（抄）の例」参照。

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、前述①と同様の取組み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。

具体的な取組みとしては、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について、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

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の取組みを実施することを契約等で確保するといった取組みが考えられます。以下では、（ｉ）の場合について有効と考えられる取組みの例を掲載します。

具体例

- 漏えいの兆候のある取引先等が製造・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、以下の取組み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
- ウィルス対策ソフト、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、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[44]。

具体例

44　ＩＰＡ『組織における内部不正防止ガイドライン』ｐ５９～ｐ６０、『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

- 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章も参照）。
- 平時から、情報漏えいを見据えた取組みを実施する。
  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、まずは以下の観点から、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

前述（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

以下に示す取組み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、コンピュータウィルス等による被害の場面では、表面的に発覚したウィ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ィルスが埋め込まれている場合もあるため、技術的専門家[45]に相談することが望まれます。

○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

○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
- 各種業法などの法令上、監督官庁等との間で、要求されている手続を実施

○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
  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
- 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。

45 http://www.ipa.go.jp/security/anshin/

（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

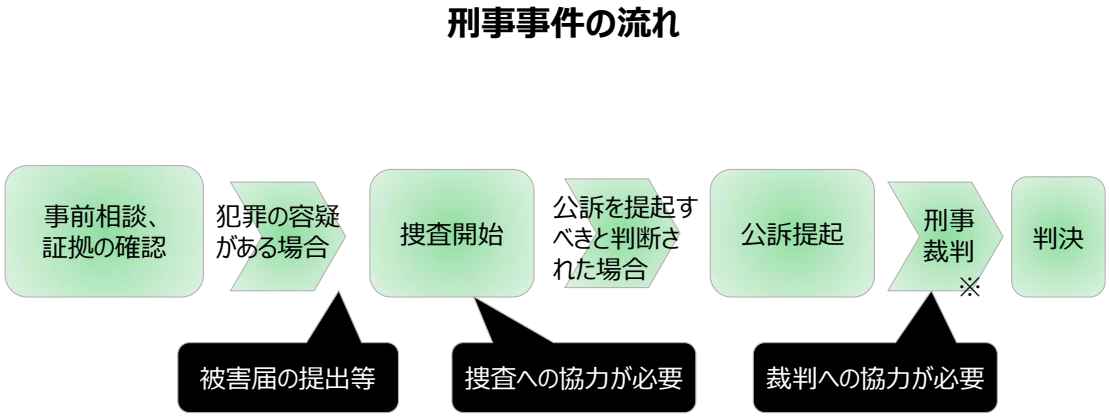
○　自社における被害回復と将来的な漏えいの抑止のため、徹底的な責任追及を実施します。

○　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、どの情報を不正競争防止法上の責任追及に係る「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

図表６（２）刑事事件の流れ



※刑事訴訟手続の流れに関しては、参考資料「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あり方について」参照。

○　秘密情報の漏えいの事案では、当該情報が営業秘密に該当した場合に不正競争防止法上の営業秘密侵害罪（同法第２１条等）に該当し得るだけではなく、不正アクセス行為の禁止等に関する法律違反の罪（同法第１１条等）、電子計算機使用詐欺罪（刑法第２４６条の２）、背任罪（同法第２４７条）、横領罪（同法第２５２条）等に該当する可能性もあります。

○　こういった罪に対する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[46]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。

相談時に持参することが望ましいと考えられる資料

- 企業の概要がわかるもの（履歴事項全部証明書、組織図、パンフレット等）
- 侵害された営業秘密がわかるもの（データ印字、簿冊のコピー等）
- 漏えいが疑われる従業員（以下「被疑者」という。）を特定する資料（履歴書、人事記録等）
- 被疑者の勤務場所がわかるもの（事務所配置図、配席図等）

46 参考資料３「各種窓口一覧」参照。

> ➢　被疑者の出退社状況がわかるもの（タイムカード、営業日誌等）
> ※６－４（２）「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」及び「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」も併せて参照。
> ※その他、コンピュータシステムの概要、職場配置図など、侵害態様の解明に役立つ資料を持参することも有用と思われる。

○　場合によっては、必要書類が整うのを待たずして、前述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り得ることに留意が必要です。

○　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）を複数回行い、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等を目指すもの。

【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（事案によっては裁判手続と同程度の期間を要する場合もある）。
- 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。なお、別途郵便切手も必要[47]）。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（担保の有無や額は裁判所が決定）が必要[48]。

【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

47 http://www.courts.go.jp/tokyo-s/saiban/l3/l4/Vcms4_00000355.html
48 http://www.courts.go.jp/tokyo-s/saiban/l3/l4/Vcms4_00000354.html

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（差止請求の有無、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み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闇雲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、本章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みとなります。

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充たす必要があります。

○　以下では、同法に規定される不正競争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。なお、これらの例は全てがそろっていないと裁判上十分な証拠とならないものではなく、あくまで有効と考えられる資料を列挙したものです。

○　いずれにせよ、証拠を収集するに当たっては、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ます。

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（教育マニュアル等）
- 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、口頭での情報管理に係る注意喚起の状況、示談文書等）

※　第３章参照

不正競争防止法違反のその他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

※　第３章参照