

退職社員による営業秘密の漏洩への実務的対応

法律事務所ASCOPE

弁護士 高橋 顕太郎

退職社員による営業秘密の漏洩への実務的対応

1. はじめに
2. 情報漏洩が問題となった事例
3. 不正競争防止法における「営業秘密」
4. 営業秘密侵害行為類型（民事）
5. 営業秘密侵害罪の類型（刑事）
6. 秘密情報漏洩の事前対策
7. 発覚時の初動対応

1. はじめに

よくあるご相談

- ◆ 同業他社に転職予定の従業員が、顧客情報を持ち出して、退職後に営業活動を行おうとしていることがわかった。
- ◆ 幹部社員が、商品に関する機密情報と主要な従業員を引き抜いて、当社と競合する会社を設立しようとしていることが発覚した。

営業秘密の漏洩への対応

- ◆ このような計画は一般的に秘密裡に実行される。
- ◆ 他方で、勧誘を受けた従業員等から情報が漏れて、経営者に事前に伝わることもある。
- ◆ そのような場合、証拠確保や被害拡大防止の観点から迅速な対応が必要であるが、労務に関する専門家として、会社に対して的確なアドバイスをするために、実際に営業秘密等の漏洩が発生した場合の「初動対応」や、事前に準備可能な「対策」を理解しておくことが重要。

1. はじめに

情報の漏洩ルート

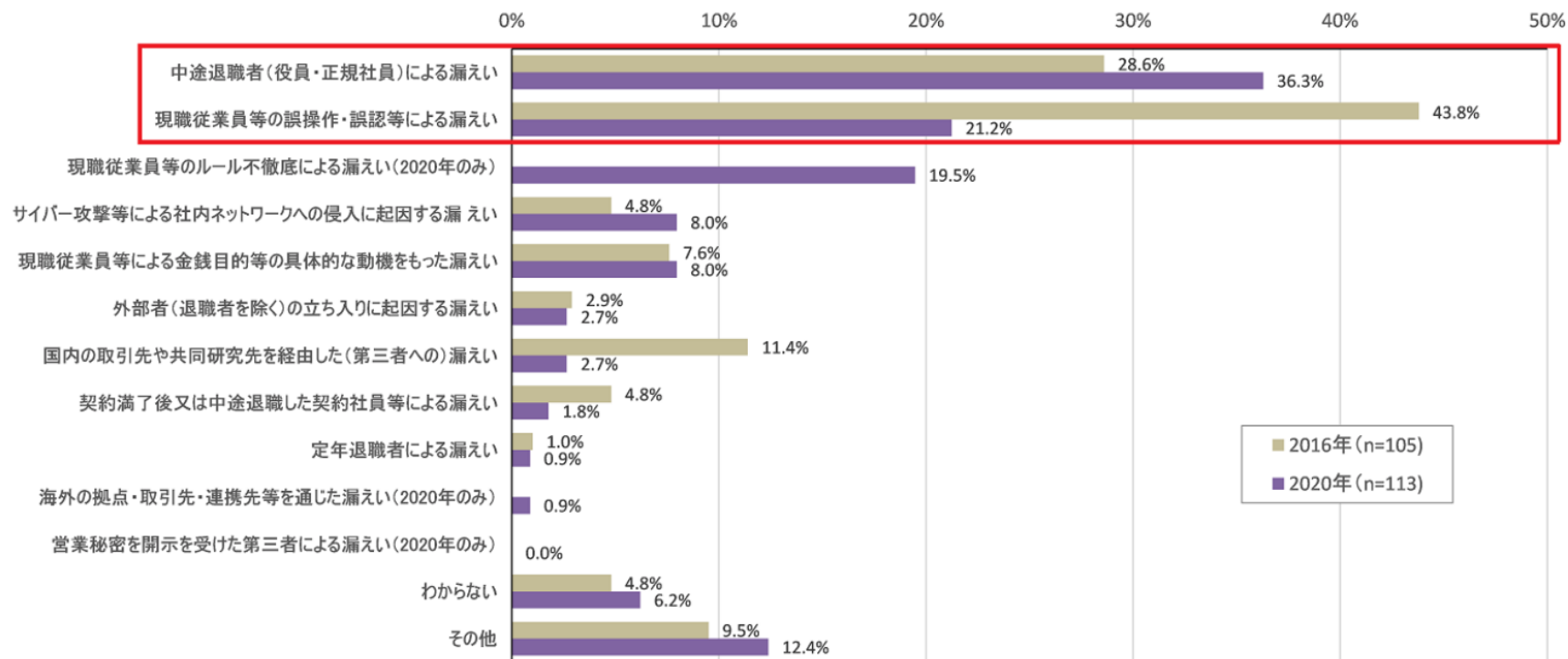


図4：営業秘密の漏えいルート

(引用元) IPA、令和2年度「企業における営業秘密管理に関する実態調査」報告書

2. 情報漏洩が問題となった事例

データ漏洩、二審も実刑判決 東芝提携先の元技術者（日経、2015.9.5）

東芝の研究データを韓国企業に渡したとして、不正競争防止法違反（営業秘密開示）の罪に問われた提携先の元技術者、杉田吉隆被告（54）の控訴審判決で、東京高裁は4日、懲役5年、罰金300万円とした一審東京地裁判決を支持し、弁護側の控訴を棄却した。

弁護側は「持ち出したフラッシュメモリーに関するデータの有用性はそれほど高くない、刑は重すぎる」と主張していた。判決理由で高裁の大島隆明裁判長は「データは、信頼性の高い製品を低コストで製造するため必要不可欠な情報だった」と指摘し、一審の量刑が不当とはいえないと判断した。

（引用元）日経新聞、2015年9月5日 1:06

https://www.nikkei.com/article/DGXLASDG04H5P_U5A900C1000000/

2. 情報漏洩が問題となった事例

5G情報持ち出し、競合他社に転職 ソフトバンク元社員に有罪判決（朝日新聞デジタル、2022.12.9）



東京地裁＝東京都千代田区 

携帯電話大手ソフトバンクの高速 移動通信方式「5G」サービスの秘密情報を社外に持ち出したとして、不正競争防止法 違反（営業秘密 の領得）の罪に問われた元社員の合場（あいば）邦章被告（47）の判決公判が9日、東京地裁（鎌倉正和裁判長）であった。判決は「転職先での職務に役立てようとした」として、懲役2年執行猶予4年、罰金100万円（求刑懲役2年罰金100万円）を言い渡した。

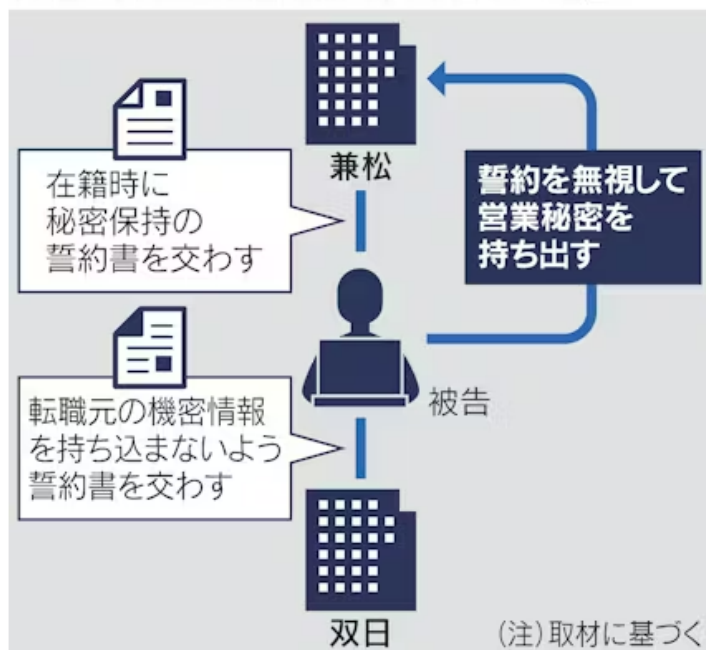
（引用元）朝日新聞デジタル、村上友里、2022年12月9日 17:57
<https://www.asahi.com/articles/ASQD95TRMQD9UTIL014.html>

2. 情報漏洩が問題となった事例

双日元社員提訴 兼松の営業秘密の持ち出し、契約書も無視（日経、2023.10.18）

東京地検は18日、転職元の兼松の営業秘密を不正取得したとして、元双日社員の眞鍋昌奨容疑者（32）を不正競争防止法違反（営業秘密侵害）罪で起訴した。被告は兼松、双日両社と秘密保持の誓約書を交わしながら約5万ファイルのデータを持ち出したことも判明した。情報流出を完全に封じるのは難しい。専門家は企業に対し、持ち出しの発生を前提とした備えの強化を求めている。

被告は両社と秘密保持の誓約書を交わしていた



(引用元) 日本経済新聞、2023年10月18日 7:14更新
<https://www.nikkei.com/article/DGXZQOUE081GO0Y3A001C2000000/>

2. 情報漏洩が問題となった事例

日本製鉄株式会社 の事案（民事）

【東京地判平成31年4月24日・知財高判令和2年1月31日】

- ◆ 方向性電磁鋼板に係る営業秘密漏えい事件で、原告日本製鉄は元従業員に対し、不正競争防止法4条等に基づく損害賠償請求を提起した事件。
- ◆ 一審の東京地裁平成31年4月24日は、営業秘密該当性を認定した後、原告の請求を全て認め、営業秘密の使用・開示の差止め、記録媒体の廃棄、10億2300万円の損害賠償等の支払いを命じた。
- ◆ 控訴審の知財高判令和2年1月31日も、控訴を棄却して、一審判決の結論を維持し、被告は個人として10億2300万円の損害賠償債務を負うこととなった。

2. 情報漏洩が問題となった事例

ベネッセコーポレーション、個人情報の漏洩

2014年6月27日、株式会社ベネッセコーポレーションは、お客様からの問い合わせによりお客様の個人情報 が社外に漏えいしている可能性を認識し、緊急対策本部を設置するとともに、これらの問い合わせ で提供された情報を手がかりとして社内調査を開始しました。

この調査により、同年7月7日、弊社からの漏えい情報であることが確認されたため、緊急対策の意思決定機関として危機管理本部を設置し、外部の情報セキュリティ専門家などを招聘し、データベースの安全確保のための緊急対策を講じ、不審な勧誘などを抑止するための活動を開始しました。

社内調査の結果、弊社の管理するデータベースから個人情報 が社外に不正に持ち出されていた事実が存在する可能性が高いことが判明したため、警察に対する相談を開始し、同年7月15日には、警視庁に対して、本件お客様情報漏えい事実についての刑事告訴を行いました。

本件刑事告訴を受け、同月17日、警視庁は、不正競争防止法違反の容疑で、弊社のシステム開発・運用を行っているグループ会社・株式会社シンフォームの業務委託先元社員を逮捕しました。

(引用元) 株式会社ベネッセコーポレーション、事故の概要

<https://www.benesse.co.jp/customer/bcinfo/01.html>

3.不正競争防止法における「営業秘密」

不正競争防止法第2条第6項

- ◆ この法律において「営業秘密」とは、①秘密として管理されている②生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、③公然と知られていないものをいう。

①秘密として管理されていること（秘密管理性）

- ◆ その情報に合法的かつ現実 접촉することができる従業員などからみて、その情報が会社にとって秘密としたい情報であることが分かる程度に、**アクセス制限**や**マル秘表示**といった秘密管理措置がなされていること。

②有用な技術上又は営業上の情報であること（有用性）

- ◆ 脱税情報や有害物質の垂れ流し情報などの公序良俗に反する情報を排除することを主眼にした要件であり、それ以外の情報であれば有用性は認められることが多い。

③公然と知られていないこと（非公知性）

- ◆ 合理的な努力の範囲内で入手可能な刊行物には記載されていないなど、保有者の管理下以外では一般に入手できないこと。

3.不正競争防止法における「営業秘密」

①秘密として管理されていること（秘密管理性）

【ベネッセ顧客情報漏えい事件・東京高裁平29.3.21判タ1443号80頁】

「当該情報に関して、その保有者が主観的に秘密にしておく意思を有しているだけではなく、当該情報にアクセスした従業員や外部者に、当該情報が秘密であることが十分に認識できるようにされていることが重要であり、そのためには、当該情報にアクセスできる者を制限するなど、保有者が当該情報を合理的な方法で管理していることが必要とされる。」と判示されている（①保有者の**秘密管理意思**だけでなく、②①に対する**従業員等の認識可能性**が必要）。

従来の考え方の変化

従来は、①情報にアクセスできる者が制限されていること（アクセス制限）、②情報にアクセスした者に当該情報が営業秘密であることが認識できるようにされていること（客観的認識可能性）の二つが判断要素になると説明されていた。しかし、現在は、両者は重要なファクターではあるが、それぞれ別個独立した要件ではなく、「アクセス制限」は「認識可能性」を担保する一つの手段と考えられており、情報にアクセスした者が秘密であることを認識できる場合には、十分なアクセス制限がないことのみを根拠に秘密管理性が否定されることはない（前掲ベネッセ顧客情報漏えい事件に同旨）。

4. 営業秘密侵害行為類型（民事）

営業秘密侵害行為（不競法第2条1項4号～10号）

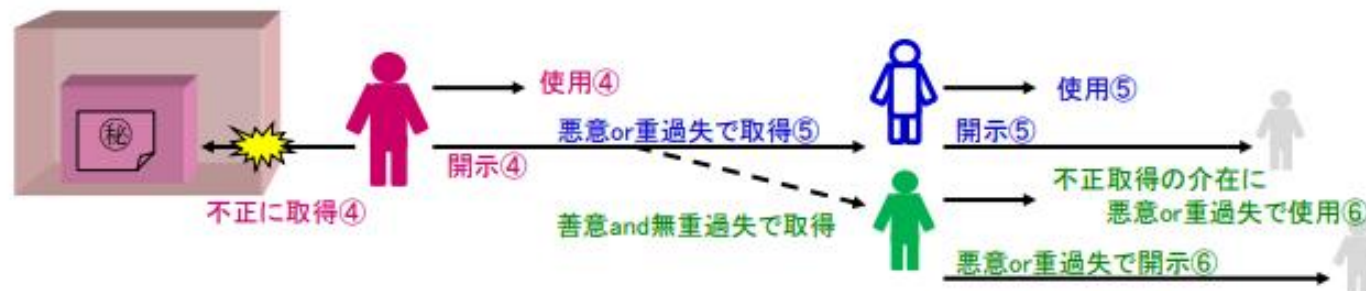
- ◆ 窃取、詐欺、強迫その他の不正の手段により営業秘密を**取得する行為**（以下「**営業秘密不正取得行為**」という。）又は営業秘密不正取得行為により取得した営業秘密を**使用し、若しくは開示する行為**（4号）
- ◆ その営業秘密について**営業秘密不正取得行為が介在したことを知って**、若しくは重大な過失により知らないで営業秘密を**取得し、又はその取得した営業秘密を使用し、若しくは開示する行為**（5号）
- ◆ その**取得した後に**その営業秘密について**営業秘密不正取得行為が介在したことを知って**、又は重大な過失により知らないでその取得した営業秘密を**使用し、又は開示する行為**（6号）
- ◆ 営業秘密を保有する事業者（以下「**営業秘密保有者**」という。）からその営業秘密を示された場合において、**不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、その営業秘密を使用し、又は開示する行為**（7号）
- ◆ その営業秘密について**営業秘密不正開示行為**であること若しくはその営業秘密について営業秘密不正開示行為が**介在したことを知って**、若しくは重大な過失により知らないで営業秘密を**取得し、又はその取得した営業秘密を使用し、若しくは開示する行為**（8号）
- ◆ その**取得した後に**その営業秘密について**営業秘密不正開示行為があったこと若しくはその営業秘密について営業秘密不正開示行為が介在したことを知って**、又は重大な過失により知らないでその取得した営業秘密を**使用し、又は開示する行為**（9号）
- ◆ 第四号から前号までに掲げる行為により**生じた物を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、輸入し、又は電気通信回線を通じて提供する行為**（10号）

※ 条文内の括弧書き部分等を適宜省略しています。

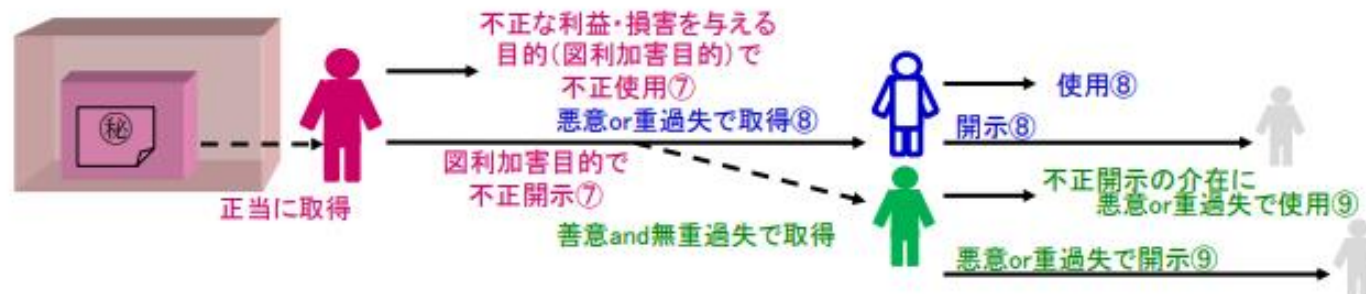
4.営業秘密侵害行為類型（民事）

営業秘密侵害行為類型（民事）

○不正取得の類型



○正当取得の類型



※ ○囲いの数字は、不正競争防止法第2条第1項各号の該当号数

※ 悪意or重過失＝当該行為があったことを知っている、あるいは重大な過失により知らない

※ 善意and無重過失＝当該行為があったことを、重大な過失なく知らない

（引用元）経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～（2024年2月）」

4. 営業秘密侵害行為類型（民事）

民事措置による責任追及

- ◆ 民事的な責任追及手段としては、当事者間の交渉による解決、民事裁判等を提起して損害賠償請求権や差止請求権を行使するという方法が考えられる。
- ◆ 裁判に先立ち、民事保全手続で裁判前に権利の確保を求めることもできる。
- ◆ 知的財産権に関する調停手続（知財調停）、ADR（裁判外紛争解決手続）の活用により、非公開の手続で柔軟な紛争解決を目指すことも考えられる。

営業秘密侵害行為に対する民事措置（裁判手続）

- ◆ 営業秘密の開示・使用の仮の差止め（保全）
- ◆ 営業秘密の使用の差止請求（訴訟）
- ◆ 営業秘密の漏洩による損害賠償請求（訴訟）

5. 営業秘密侵害罪の類型（刑事）

営業秘密侵害罪（不競法 2 1 条 1 項） ※令和 6 年 4 月に改正法施行

次の各号のいずれかに該当する場合には、当該違反行為をした者は、**十年以下の懲役若しくは二千万円以下の罰金**に処し、又はこれを併科する（同法 2 1 条 1 項）。

- ◆ **不正の利益を得る目的**で、又はその**営業秘密保有者に損害を加える目的**で、**詐欺等行為又は管理侵害行為**により、**営業秘密を取得**したとき（**1 号**）
- ◆ **詐欺等行為又は管理侵害行為**により取得した営業秘密を、**不正の利益を得る目的**で、又はその**営業秘密保有者に損害を加える目的**で、**使用し、又は開示**したとき。（**2 号**）
- ◆ **不正の利益を得る目的**で、又はその**営業秘密保有者に損害を加える目的**で、前号若しくは次項第二号から第四号までの罪、第四項第二号の罪（前号の罪に当たる開示に係る部分に限る。）又は第五項第二号の罪に当たる開示によって**営業秘密を取得**して、その営業秘密を**使用し、又は開示**したとき。（**3 号**）
- ◆ **不正の利益を得る目的**で、又はその**営業秘密保有者に損害を加える目的**で、前二号若しくは次項第二号から第四号までの罪、第四項第二号の罪（前二号の罪に当たる開示に係る部分に限る。）又は第五項第二号の罪に当たる開示が**介在したことを知って**営業秘密を取得して、その営業秘密を**使用し、又は開示**したとき。（**4 号**）
- ◆ **不正の利益を得る目的**で、又はその**営業秘密保有者に損害を加える目的**で、自己又は他人の第二号から前号まで又は第四項第三号の罪に当たる行為（技術上の秘密を使用する行為に限る。以下この号において「違法使用行為」という。）により**生じた物を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、輸入し、又は電気通信回線を通じて提供**したとき。（**5 号**）

※ 条文内の括弧書き部分等を適宜省略しています。

5. 営業秘密侵害罪の類型（刑事）

営業秘密侵害罪（不競法 2 1 条 2 項） ※令和 6 年 4 月に改正法施行

次の各号のいずれかに該当する者は、**十年以下の拘禁刑若しくは二千万円以下の罰金**に処し、又はこれを併科する（同法 2 1 条 2 項）。

- ◆ **営業秘密を営業秘密保有者から示された者**であって、**不正の利益を得る目的**で、又はその**営業秘密保有者に損害を加える目的**で、その営業秘密の管理に係る**任務に背き**、次のいずれかに掲げる方法でその営業秘密を**領得**したもの（**1号**）
 - イ 営業秘密記録媒体等又は営業秘密が化体された物件を**横領**すること。ロ 営業秘密記録媒体等の記載若しくは記録について、又は営業秘密が化体された物件について、その**複製を作成**すること。ハ 営業秘密記録媒体等の記載又は記録であって、消去すべきものを消去せず、かつ、当該記載又は記録を**消去したように仮装**すること
- ◆ **営業秘密を営業秘密保有者から示された者**であって、その営業秘密の管理に係る任務に背いて前号イから八までに掲げる方法により領得した営業秘密を、**不正の利益を得る目的**で、又はその**営業秘密保有者に損害を加える目的**で、その営業秘密の管理に係る**任務に背き、使用し、又は開示**したもの（**2号**）
- ◆ **営業秘密を営業秘密保有者から示されたその役員又は従業者**であって、**不正の利益を得る目的**で、又はその**営業秘密保有者に損害を加える目的**で、その営業秘密の管理に係る**任務に背き**、その営業秘密を**使用し、又は開示**したもの。（**3号**）
- ◆ **営業秘密を営業秘密保有者から示されたその役員又は従業者であつた者**であって、**不正の利益を得る目的**で、又はその**営業秘密保有者に損害を加える目的**で、その在職中に、その営業秘密の管理に係る任務に背いてその営業秘密の開示の**申込み**をし、又はその営業秘密の使用若しくは開示について**請託を受けて**、その営業秘密をその職を退いた**後に使用し、又は開示**したもの。（**4号**）
- ◆ **不正の利益を得る目的**で、又はその**営業秘密保有者に損害を加える目的**で、自己又は他人の第二号から前号まで又は第五項第三号の罪に当たる行為により**生じた物を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、輸入し、又は電気通信回線を通じて提供した者**（**5号**）

※ 条文内の括弧書き部分等を適宜省略しています。

5. 営業秘密侵害罪の類型（刑事）

営業秘密侵害罪の類型（刑事）（第21条第1項、第3項）①

○不正な手段（詐欺・恐喝・不正アクセスなど）による取得のパターン

（1号）図利加害目的で、詐欺など行為又は管理侵害行為によって、営業秘密を不正に取得する行為



詐欺など行為・管理侵害行為により、
営業秘密を不正に取得①

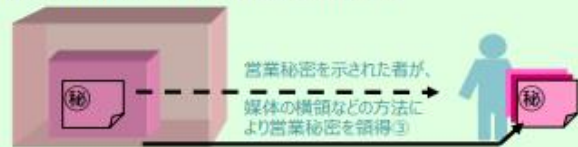
（2号）不正に取得した営業秘密を、図利加害目的で、使用又は開示する行為



詐欺など行為・管理侵害
行為により不正に取得

○正当に営業秘密が示された者による背信的行為のパターン

（3号）営業秘密を保有者から示された者が、図利加害目的で、その営業秘密の管理に係る任務に背き、（イ）媒体などの横領、（ロ）複製の作成、（ハ）消去義務違反＋仮装、のいずれかの方法により営業秘密を領得する行為



営業秘密を示された者が、
媒体の横領などの方法により
営業秘密を領得③

（4号）営業秘密を保有者から示された者が、第3号の方法によって領得した営業秘密を、図利加害目的で、その営業秘密の管理に係る任務に背き、使用又は開示する行為



営業秘密を示された者が、
3号の方法により営業秘密を領得

（5号）営業秘密を保有者から示された現職の役員又は従業員が、図利加害目的で、その営業秘密の管理に係る任務に背き、営業秘密を使用又は開示する行為



在職中に営業秘密を既に
示されている者

（6号）営業秘密を保有者から示された退職者が、図利加害目的で、在職中に、その営業秘密の管理に係る任務に背いて営業秘密の開示の申込みをし、又はその営業秘密の使用若しくは開示について請託を受け、退職後に使用又は開示する行為



在職中に営業秘密を既に
示されている者

在職中に「図利加害目的」で使用・開示の約束

【旧法⇒新法】

21条1項1号⇒21条1項1号

21条1項2号⇒21条1項2号

21条1項3号⇒21条2項1号

21条1項4号⇒21条2項2号

21条1項5号⇒21条2項3号

21条1項6号⇒21条2項4号

21条1項7号⇒21条1項3号

21条1項8号⇒21条1項4号

21条1項9号⇒21条1項5号

21条3項⇒21条4項、5項

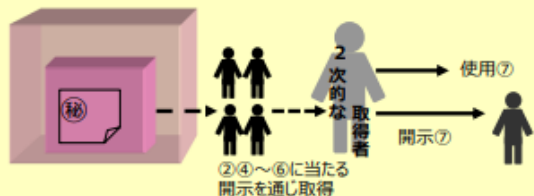
（引用元）経済産業省「不正競争防止法の概要（2022年）」

5. 営業秘密侵害罪の類型（刑事）

営業秘密侵害罪の類型（刑事）（第21条第1項、第3項）②

○転得者による使用・開示のパターン

（7号）図利加害目的で、②、④～⑥の罪に当たる開示（海外重罰の場合を含む）によって取得した営業秘密を、使用又は開示する行為（2次的な取得者を対象）



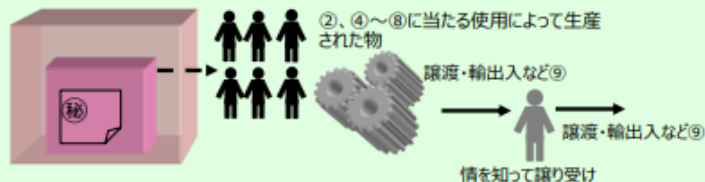
（8号）図利加害目的で、②、④～⑦の罪に当たる開示（海外重罰の場合を含む）が介在したことを知って営業秘密を取得し、それを使用又は開示する行為（3次以降の取得者をすべて対象）



※3次以降の取得者までの転々流通の過程で悪意者が存在したとしても、当該3次以降の取得者が、いずれかの者による「不正な開示」が介在したことを知って取得し、不正使用・開示した場合は、処罰対象となり得る。

○営業秘密侵害品の譲渡などのパターン

（9号）図利加害目的で、②、④～⑧の罪に当たる使用（海外重課の場合を含む）によって生産された物を、譲渡・輸出入する行為



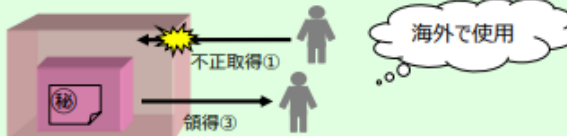
刑事規定（第21条第1項、第3項）

罰 則：10年以下の懲役若しくは2000万円以下の罰金（又はこれの併科）
法人両罰は5億円以下の罰金（第22条第1項第2号）
※海外使用などは個人が3000万円以下、法人は10億円以下。

（引用元）経済産業省「不正競争防止法の概要（2022年）」

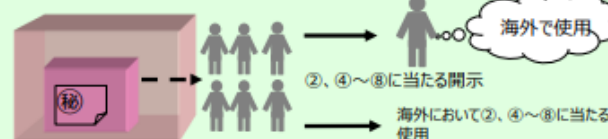
○海外重罰のパターン（21条3項）

（1号）日本国外で使用する目的での①又は③の行為



（2号）日本国外で使用する目的を持つ相手方に、それを知って②、④～⑧に当たる開示をする行為

（3号）日本国外で②、④～⑧に当たる使用をする行為



【旧法⇒新法】

21条1項1号⇒21条1項1号

21条1項2号⇒21条1項2号

21条1項3号⇒21条2項1号

21条1項4号⇒21条2項2号

21条1項5号⇒21条2項3号

21条1項6号⇒21条2項4号

21条1項7号⇒21条1項3号

21条1項8号⇒21条1項4号

21条1項9号⇒21条1項5号

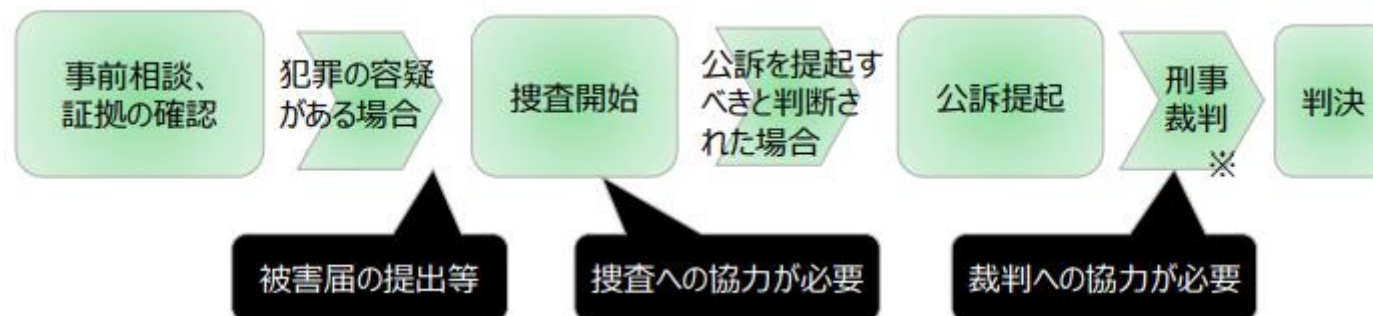
21条3項⇒21条4項、5項

5. 営業秘密侵害罪の類型（刑事）

刑事手続による責任追及

- ◆ 将来的の再発防止のためには、徹底的な責任追及を考える必要がある。
- ◆ 刑事と民事のいずれの措置（又は双方の措置）を採るかは、具体的事情に応じて臨機応変に検討する。

刑事事件の流れ



（引用元）経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～（2024年2月）」

5. 営業秘密侵害罪の類型（刑事）

営業秘密侵害行為に対する刑事措置の例

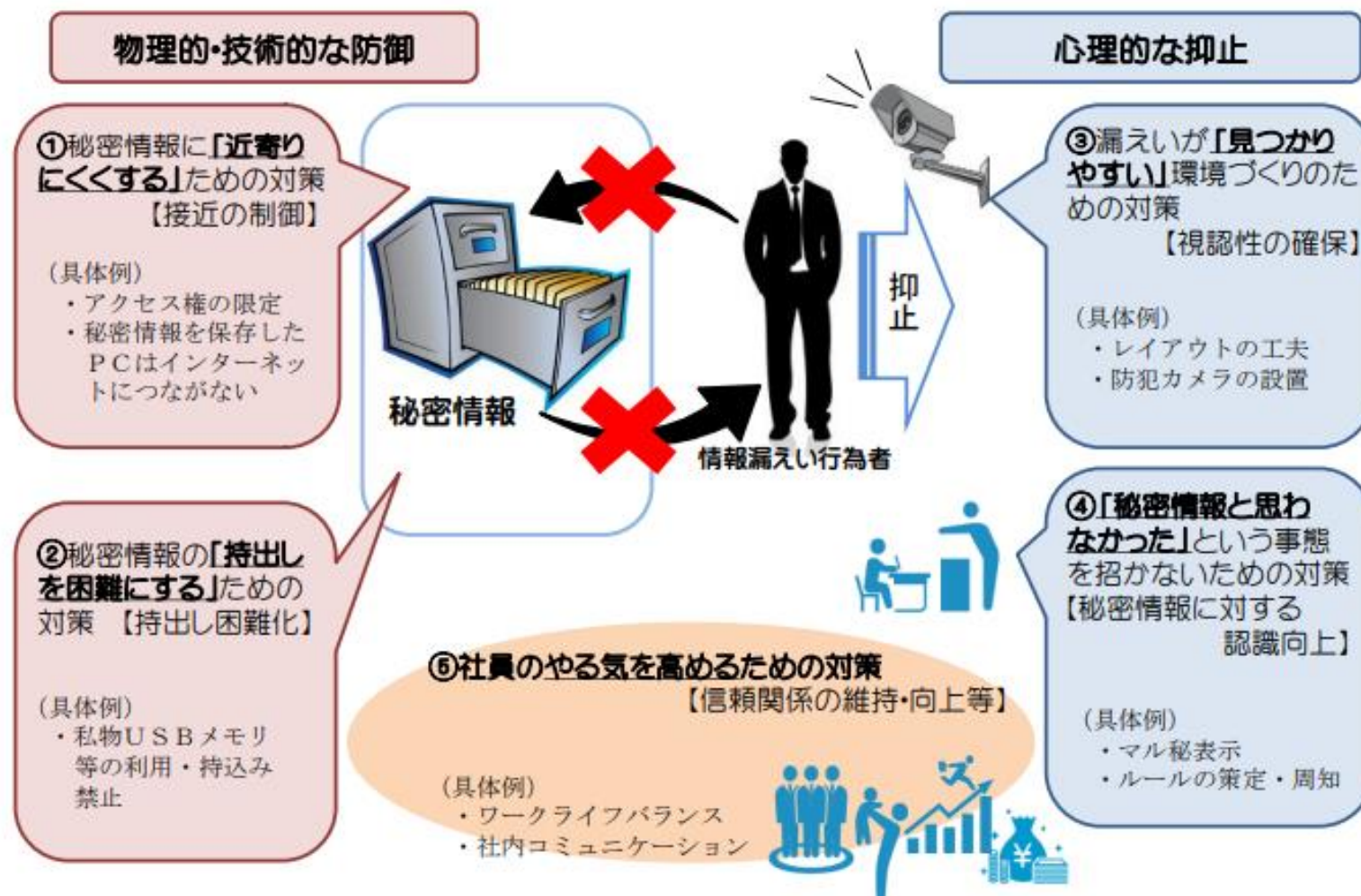
- ◆ 不正競争防止法上の営業秘密侵害罪（不競法第21条等）
- ◆ 不正アクセス行為の禁止等に関する法律違反の罪（不競法第11条等）
- ◆ 電子計算機使用詐欺罪（刑法第246条の2）
- ◆ 背任罪（刑法第247条）
- ◆ 横領罪（刑法第252条）
- ◆ 個人情報データベース等不正提供罪（個人情報保護法第179条）

など

➡どの法令に基づき被害届や刑事告訴を行うかについては、具体的な事実や収集できた証拠等によって検討が必要となる。

6. 秘密情報漏洩の事前対策

情報漏洩の5つの「対策の目的」



(引用元) 経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～(2024年2月)」

6. 秘密情報漏洩の事前対策

(1) 「接近の制御」からの対策

◆ 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を明確にするなど。

◆ 情報システムにおけるアクセス権者のID登録

- ・ 従業員が情報システムへアクセスする際に、IDとパスワードによる認証を徹底する。

◆ 分離保管による秘密情報へのアクセス制限

- ・ 秘密情報が記録された書類・ファイル等は、他の情報と、保管する書棚や格納するサーバを分離する。

◆ ペーパーレス化

- ・ 秘密情報をペーパーレスにし、電子データには印刷やコピーに制限を加え、アクセスする機会を減少させる。

◆ 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や、電子データの消去を行う場合、復元して当該情報にアクセスできない様に復元不可能な状態にして廃棄・消去する。

6. 秘密情報漏洩の事前対策

(2) 「持出し困難化」からの対策

◆ 書類、記録媒体、物自体等の持出しを困難にする措置

- ・ 会議資料の適切な回収、PCの持ち出し制限、電子データの暗号化、遠隔操作によるデータ消去機能の導入など。

◆ 電子データの外部送信による持出しを困難にする措置

- ・ 社外へのメール送信・WEBアクセス制限、許可したソフトウェア以外のインストール禁止など。

◆ 秘密情報の複製を困難にする措置

- ・ コピー防止用紙やコピーガード付の記録媒体の使用、私物のUSBメモリ・携帯電話等の利用・持ち込み制限など。
- ・ リモートワークでは、自宅で用いるPC等に電子データを可能な限り保存させない、NDR（Network Detection and Response）等の導入で社内ネットワーク全体の不審な挙動や異常を検知し、操作・送信履歴を確保するなど。

◆ 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

- ・ 秘密情報に触れるプロジェクトに参加する際に、就業規則等とは別に**秘密保持契約書等**を締結し、対象となる秘密情報を明確化した上で、プロジェクト終了時に書類等を返還、消去させる。

6. 秘密情報漏洩の事前対策

(3) 「視認性の確保」からの対策

◆ 管理の行き届いた職場環境を整える対策

- ・書類等の整理整頓、**秘密情報の管理に関する責任の分担**、「写真撮影禁止」・「関係者以外立入り禁止」の表示など。

◆ 目につきやすい状況を作り出す対策

- ・職場の座席配置・レイアウトの変更により死角をなくす。防犯カメラの設置など。
- ・外部へ送信するメールを上司が承認又はCCに入れる設定にする。
- ・情報漏洩に関する内部通報窓口・匿名での私書箱の設置など。

◆ 事後的に検知されやすい状況を作り出す対策

- ・秘密情報が記録された媒体の管理（通し番号管理）、印刷者の氏名等が透かしで印刷される設定の導入など。
- ・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。
- ・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。
- ・秘密情報の管理の実施状況や情報漏洩行為の有無等に関する定期・不定期での監査とその周知。

6.秘密情報漏洩の事前対策

(4) 「秘密情報に対する認識向上」からの対策

◆ 秘密情報の取扱い方法等に関するルールの周知

- ・秘密情報の取扱いに関する社内規程の従業員への周知徹底及び継続的な研修等（資料配布や会議）の実施。

◆ 秘密保持契約等（誓約書を含む）の締結

- ・秘密情報を取り扱う従業員等と秘密保持に関する契約書や誓約書を締結する。
- ・研修等の実施後に「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」との誓約書を取得する。

◆ 秘密情報であることの表示

- ・秘密情報が記載された媒体に「マル秘」「役員限り」「持出し禁止」などの取扱い方法を明記する。
- ・秘密情報が記録された媒体等を保管する書庫や区域に「無断持出し禁止」といった掲示を行う。
- ・秘密情報であることの表示が困難なものについては、秘密情報物件リストを作成して周知を行う。

6.秘密情報漏洩の事前対策

(5) 「信頼関係の維持・向上等」からの対策

◆ 秘密情報の管理に関する従業員等の意識向上

- ・ 秘密情報の管理の実践例とその企業への貢献を周知して、秘密情報の管理の重要性に関する理解を深める。
- ・ 情報漏洩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、具体的な事例を準備して説明する。
- ・ 情報漏洩事案に対して、社内で **どのような処分がなされるのか予め説明** しておく。

◆ 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

- ・ 働きやすい職場環境の整備
- ・ 透明性が高く公平な **人事評価制度の構築・周知**

6. 秘密情報漏洩の事前対策

労務の専門家としての具体的な対応

◆ 秘密情報の取扱いに関する社内規程の整備

- ・就業規則、情報管理規程、テレワーク勤務規程などに、秘密情報の管理を適切に行うための条項を追加する。

◆ 規程に盛り込むべき条項

- ・**適用範囲**：役員、従業員、派遣社員、委託先従業員（自社内勤務の場合）など適用範囲を明確にする。
- ・**秘密情報の定義**：規程の対象となる情報の定義を明確化する。
- ・**秘密情報の分類**：「役員外秘」、「部外秘」、「社外秘」のような分類と、その分類の対象となる秘密情報
- ・**分類ごとの対策**：「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しを禁止する」、「私物のUSBメモリの持込みを制限し複製を禁止する」など分類ごとに講ずる対策を記載する。
- ・**管理責任者**：秘密情報の管理を統括する者を規定する。
- ・**秘密上及びアクセス権の指定に関する責任者**：分類ごとに秘密情報の指定やアクセス権の付与を実施する責任者を規定する。
- ・**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を規定する。
- ・**罰則**：秘密情報を漏洩した場合の罰則を規定する。

6. 秘密情報漏洩の事前対策

秘密情報管理に関する就業規則の例

第●条（遵守事項）

従業員は、次の各号に定める事項を守らなければならない。

- ・ 従業員は、秘密情報管理規程に従い、秘密情報の取扱いを遵守しなければならない。
- ・ 会社の内外を問わず、在職中、又は退職若しくは解雇によりその資格を失った後も、会社の秘密情報を、不正に開示したり、不正に使用したりしないこと。
- ・ 退職時に、会社から貸与されたパソコンや携帯電話等、会社から交付を受けた資料（紙、電子データ及びそれらが保存されている一切の媒体を含む）を全て会社に返却すること。
- ・ 会社の許可なく、立入禁止区域に立ち入り、又は業務外の事由で自己の職場以外に立ち入り、若しくは会社の施設・敷地を利用しないこと。
- ・ 会社の許可なく、会社の秘密情報を無断で社外に持ち出さないこと。
- ・ 業務上知った会社の秘密情報を使用し、在職中又は退職後においてその公表前に直接若しくは間接的に関連株式の売買を行わないこと。

（参照）経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～（2024年2月）」

6. 秘密情報漏洩の事前対策

秘密情報管理に関する就業規則の例

第●条（電子メール・インターネット等の適正利用）

1. 従業員は、会社の電子メール、イントラネット及びインターネット（以下、総じて「インターネット等」という。）の利用に関し、次の事項を遵守して、パソコン、スマートフォン、携帯電話その他の情報通信機器（以下、総じて「端末」という。）を使用し、適切な情報ネットワーク環境の維持並びに社内情報の毀損及び漏えいの防止に努めなければならない。
 - ・ 会社が従業員に貸与した端末を業務以外の目的で使用しないこと。
 - ・ 私物の端末を会社の許可なく業務目的で使用しないこと。
 - ・ 会社が指定したウィルス対策ソフトを適正に運用、使用すること。
 - ・ 会社の内外を問わず、業務に使用する端末において、ファイル交換ソフトその他の情報管理上問題が発生する可能性があるソフトウェア等又は業務に関係のないソフトウェア等をインストールしないこと。
 - ・ 会社の許可なく、私物のU S Bメモリ、ハードディスク等の記録媒体又は私物の端末を、業務に利用する端末に接続しないこと。
 - ・ 前項の許可を得て接続する場合は、アクセス権限のない者が操作できないようにパスワード設定をすること。
 - ・ 業務に関係のないW E Bサイトにアクセスしないこと。

（参照）経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～（2024年2月）」

6. 秘密情報漏洩の事前対策

秘密情報管理に関する就業規則の例

第●条（電子メール・インターネット等の適正利用）

2. 会社は、インターネット等の利用の適正化を図るため、及び会社の秘密情報の管理を図るため、次の各号に定める事項その他必要と認める事項を講ずることができる。

- ・ 必要に応じて、会社が従業員に貸与した端末若しくは会社のサーバに保存されているデータを閲覧し、又は、情報を解析し、従業員ごとのインターネット等の利用履歴を確認すること。
- ・ 必要に応じて、従業員が送受信した社用電子メールの内容を閲覧すること。
- ・ ウィルス感染等を予防するため、特定のWEBサイトへのアクセスを制限すること。

（参照）経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～（2024年2月）」

6. 秘密情報漏洩の事前対策

秘密情報管理に関する就業規則の例

第●条（防犯カメラの設置等）

1. 会社は、会社の防犯及び秘密情報の管理のため、次の各号に定める場所その他必要と認める場所に、防犯カメラを設置し、撮影することができる。
 - ・ 敷地出入口
 - ・ サーバルーム出入口及び同ルーム内
 - ・ （略）
2. 会社は、次の各号に定める場合その他必要と認める場合には、防犯カメラにより撮影された画像又は動画の閲覧、保存等を行うことができる。
 - ・ 不法侵入者のあった場合
 - ・ （略）

（参照）経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～（2024年2月）」

6. 秘密情報漏洩の事前対策

秘密情報管理規程の例

第3条（定義）

この規程において各用語の定義は、次に定めるところによる。

- ① 「秘密情報」とは、会社が保有する情報のうち、第●条の規定により、秘密として保持すべきと決定した情報、又は同条の規定による秘密として保持すべきと決定をしていない情報であって、当該情報の内容、性質及び管理態様等から会社が秘密であることを認識できるもので不正競争防止法第2条第6項に規定する営業秘密に該当する情報をいう。
- ② 「文書等」とは、文書、図画、写真、ストレージ（フラッシュメモリ（SSD、USBメモリ、SDカードなど）、光学ディスク（CD、DVD、ブルーレイディスクなど）、磁気ディスク（ハードディスクなど以下「ストレージ」という。）等の記録媒体に情報を記載又は記録したものをいう。
- ③ 「電子化情報」とは、ストレージやオンラインストレージ（クラウドサービス等）に電磁的に記録される情報であって、情報システムによって処理が可能な形態にあるものをいう。
- ④ 「物件」とは、物品、製品、設備その他の文書等以外のものをいう。

（参照）経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～（2024年2月）」

6. 秘密情報漏洩の事前対策

秘密情報管理規程の例

第4条（秘密情報の分類）

秘密情報として管理するため、次のとおり分類を定める。

- ① 極秘 これを他に漏らすことにより会社が極めて重大な損失若しくは不利益を受ける、又はそのおそれがある秘密情報であり、原則として指定された者以外には開示してはならないもの。
- ② 社外秘 極秘以外の秘密情報であり、原則として社内の者以外には開示してはならないもの。
- ③ （略）

第9条（秘密保持義務）

- 1. 従業員等は、管理責任者の許可なく、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。
- 2. 従業員等は、管理責任者の許可なく、秘密情報を指定された業務以外の目的で使用してはならない。

第18条（罰則）

従業員等が故意又は重大な過失により、この規程に違反し、就業規則に定める各種懲戒に該当する場合は、同規則により処罰される。

（参照）経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～（2024年2月）」

6. 秘密情報漏洩の事前対策

秘密保持に関する誓約書の例（プロジェクト参加時）

第1条（秘密保持の誓約）

会社の許可なく、本プロジェクトに関して会社が秘密情報として指定した情報（以下「対象秘密情報」という。）を、本プロジェクトの参画者以外の者に対し開示し、又は本プロジェクト遂行の目的以外に使用しないことを約束いたします。

第2条（プロジェクト終了後の秘密保持等）

1. 対象秘密情報を、公知になったものを除き、本プロジェクト終了後（退職後も含む。）も、不正に開示又は不正に使用しないことを約束いたします。
2. 本プロジェクトを終了するとき、本プロジェクトを担当しなくなったとき、又は会社による要求があるときには、対象秘密情報が記録等された会社の文書等（文書、図画、写真、USBメモリ、DVD、ハードディスクドライブその他の情報を記載又は記録するものをいう。以下同じ。）又は物件であって自己の保管するものを、遅滞なくすべて会社に返還し、その旨書面にて報告いたします。
3. 前項に定める場合において、対象秘密情報が自己の文書等に記録等されているときには、当該情報を消去するとともに、消去した旨（自己の文書等に対象秘密事項が記録等されていないときは、その旨）、書面にて報告いたします。

（参照）経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～（2024年2月）」

6. 秘密情報漏洩の事前対策

秘密保持に関する誓約書（プロジェクト参加時）の例

第3条（第三者に対する守秘義務の遵守）

第三者に対して守秘義務を負っている情報については、本プロジェクトにおいて知り得たかそれ以前から知っていたかにかかわらず、その守秘義務を遵守することを約束いたします。

第4条（情報の帰属）

本プロジェクトの業務の成果である情報は会社に帰属することを確認し、異議を述べません。

以上

（参照）経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～（2024年2月）」

6. 秘密情報漏洩の事前対策

転職者採用時に取得する誓約書の例

第●条（在職時の秘密保持）

就業規則、秘密情報管理規程を遵守し、次に示される貴社の企業秘密（営業秘密を含む。以下、同じ。）について、貴社の許可なく、不正に開示又は使用しないことを約束いたします。

- ① 製品開発に関する技術資料、製造原価及び販売における価格決定等の製品に関する情報
- ② （略）

第●条（第三者の企業秘密）

1. 第三者の企業秘密を含んだ媒体（文書、写真、USBメモリ、DVD、ハードディスクドライブ、その他記録媒体等の資料及びそれらの複製物及び業務に関連して取得した名刺等すべての資料）を一切保有しておらず、また今後も保有しないことを約束いたします。
2. 貴社の業務に従事するにあたり、第三者が保有するあらゆる企業秘密を、当該第三者の事前の書面による承諾なくして貴社に開示し、又は使用若しくは出願させない、貴社が使用等するように仕向けない、または貴社が使用等していると見なされるような行為を貴社に取らせないことを約束いたします。

（参照）経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～（2024年2月）」

7. 発覚時の初動対応

漏洩事案への対応の考え方

- ◆ 企業が情報管理を徹底していても、情報漏洩の手口の高度化等を考えると、事前の準備により情報漏洩を完全に防ぐことは困難。
- ◆ そのため、万が一情報漏洩が怒った場合に迅速に対応できるように備えておくことが重要。

(1) 漏洩の兆候の把握

- ◆ 秘密情報を保管しているサーバや記録媒体へのアクセス回数の大幅な増加
- ◆ 業務上必要のないアクセス行為
- ◆ 退職前の社内トラブルの存在
- ◆ 在職時の他社との関係（転職の勧誘を受けていたなど）
- ◆ 競合他社への転職（転職後に競合他社が類似商品を販売など）

7. 発覚時の初動対応

(2) 漏洩の疑いの確認

- ◆ 兆候を確認した場合に放置せずに、初動対応を開始すべきか確認が必要。
- ◆ 業務に伴うアクセスログを確認する。
 - ・ 秘密情報へのアクセス履歴、利用者の操作履歴（メールの送受信）、クラウドサービスのログイン履歴など
 - ・ テレワークの場合には、VPN装置へのアクセス履歴やテレワーク関連機器への操作履歴など
- ◆ モニタリングシステムの活用。
 - ・ AI等の最新技術を組み入れたモニタリングシステムの活用も考えられる。
- ◆ メールモニタリングや社内PCのログ確認については、従業員の個人情報保護の観点から、かかる措置を行う場合には、事前に就業規則等で定めておくべき。

7.発覚時の初動対応

(3) 初動対応

◆ 社内調査・状況の正確な把握・原因究明

- ・「いつ、だれが、なにを、どのように」の観点から、現時点で把握できていること、できていないことを社内で明らかにする。

◆ 被害の検証

- ・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、どのような損失が予測されるか、最悪の事態を想定して検証を行う。

◆ 初動対応の観点

- ・更なる拡散の防止（漏洩した者に対する警告書の発出など）
- ・法律に基づく手続（個人情報漏洩の場合➡個人情報保護委員会への報告・法26条）
- ・企業イメージを含む損失の最小化
 - 把握している事実に基づき、速やかな対外公表
 - 顧客名簿流出時の被害者対応・マスコミ対応

（参照）経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～（2024年2月）」

7.発覚時の初動対応

+α 初動対応（実務対応の観点から）

◆ 初動対応の観点

- ・ 情報を持ち出そうとする者は、自らの行為が違法行為であることを認識しているため、会社にばれないように用意周到に行っており、退職の際にはメール履歴や貸与PCのデータを完全に削除していることが多い。
- ・ 事前準備でアクセスログ等を残せていればいいが、中小企業では事前準備ができておらず、情報を持ち出された後に漏洩の証拠を確保することは非常に難しい。
- ・ そこで、情報漏洩の疑いが生じた場合には、なによりも証拠確保が大事。

◆ 証拠確保・漏洩防止の方法

- ・ 社内システムのアクセスログや防犯カメラ映像などの記録を保全する。
- ・ LINEやChatの証拠がある場合には、スクリーンショットで証拠を残す。
- ・ 業務用PC・携帯を回収する（退職まで待つと削除されるリスクあり）。
- ・ 自宅待機を命じて、社内システムへのアクセス権をはく奪する。
- ・ 取引先へのヒアリング、調査への協力要請など

最後に

営業秘密漏洩の事案については、疑いが発生し、そこから相談する専門家（弁護士等）を探しているうちに、情報を持ち出されてしまったり、証拠隠滅を図られてしまったりし、手遅れになってしまうケースも多い印象があります。

従業員の側もニュース等で営業秘密の漏洩に対して重い刑事罰が科されていることを知り、手口が巧妙になってきています。

営業秘密の漏洩については、社労士の先生方の主たる相談内容ではないかもしれませんが、社内規程の整備を行う際などに、合わせて営業秘密漏洩への事前対策を行っていただくことや、初動対応で適切なアドバイスにより証拠の確保ができることで、被害を最小限に抑えることもできると思います。