

岩田合同法律事務所 ニュースレター
2025 年 12 月

危機管理



営業秘密の持ち出しに関する危機管理

弁護士 齋藤 弘樹

サイバー攻撃による情報漏えい事案に対する危機管理の重要性が増していますが、その一方で従業員等による情報持ち出し事案の危機管理も引き続き重要です。本稿では情報持ち出しに関する法律の概要をご説明した上、特に刑事事件の手続に焦点を当てて解説をしていきます。

1 情報持ち出しと不正競争防止法

企業の保有する情報が持ち出された場合の民事上及び刑事上の法律関係については、不正競争防止法（以下「法」といいます。）が定めており、「営業秘密」の持ち出しがなされると、持ち出しをした者だけでなく、これを転得した者（営業秘密の開示を受けた者、持ち込まれた者）においても民事・刑事両方の責任が生じます。

具体的な禁止行為の内容は経済産業省がまとめた資料^[1]^[2]が参考になりますが、本稿でも概要をご説明します。

（１）民事上の問題

ア 持ち出した者

持ち出した者については、以下の行為をした場合に民事上の損害賠償請求や差止請求の対象となります。

¹ 経済産業省が 2025 年 6 月に公開した「不正競争防止法テキスト」
(https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/unfaircompetition_textbook.pdf)

² 経済産業省が 2024 年 4 月に公開した「逐条解説 不正競争防止法」
(<https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/Chikujo.pdf>)

- ① 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・使用・開示する行為（法 2 条 1 項 4 号）
- ② 営業秘密保有（＝営業秘密を保有する企業のこと）者から営業秘密を示された者であっても、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・開示する行為（法 2 条 1 項 7 号）

イ 転得した者

転得した者については、一定の行為をした場合に民事上の損害賠償請求や差止請求の対象となり^[3]、転職者を受け入れる企業等の立場からすれば注意が必要です。

（2）刑事上の問題

ア 持ち出した者

持ち出した者については、以下の行為をした場合に刑事罰の対象となります。

- ① 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（以下「図利加害目的」といいます。）で詐欺・恐喝・不正アクセスなどにより取得・使用・開示する行為（法 21 条 1 項 1 号、2 号）
- ② 営業秘密を営業秘密保有者から示された者による背信的な行為^[4]（法 21 条 2 項 1 号～4 号）

イ 転得した者

転得した者について見ると、図利加害目的の下、上記①②の開示によって営業秘密を取得する行為や取得後に使用・開示する行為（法 21 条 1 項 3 号）も刑事罰の対象となります。営業秘密を持ち込んだ転職者から開示を受けた企業の役職員も刑事罰の対象となり得る（そして両罰規定により企業自体も刑事罰の対象となり得る）ことに注意が必要です。

（3）秘密管理性、有用性、非公知性

不正競争防止法上、上記で説明した民事上・刑事上の責任が生じるのは「営業秘密」の取得等に限られます。「営業秘密」該当性が認められるためには①秘密管理性、②有用性、③非公知性の 3 つを充足することが必要となります。

②は公序良俗に反する内容の情報を法律上の保護の範囲から除外することに主眼を置いた要件であり、それ以外の情報であれば有用性が認められることが多いとされ、③については、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を指し、公知情報の組合せであっても、その組合せの容易性やコストに鑑み非公知性が認められ得るとされています。^[5]

一方、①については、経済産業省により、不正競争防止法により営業秘密として法的保護

³ 場合分けや例外規定もありますので、本稿では説明を割愛します。脚注 1 の 25 頁をご参照ください。

⁴ 法 21 条 2 項 1 号から 4 号に具体的な行為類型が定められています。

⁵ 脚注 1 の 22 頁参照。

を受けるために必要となる「最低限の水準の対策」が示されていますが^[6]、この最低限の水準の対策さえ実施されておらず、営業秘密該当性が否定されるケースも少なくありません。

2 刑事事件例

大規模な情報持ち出し事案につき、刑事事件判決が出された例として以下のようなものがあります。③のように長期間情報の持ち出しを繰り返した上、業者に情報を売却していたような事例でも執行猶予付き判決に留まることもあります。また、企業としては刑事事件化するか否かを問わず、実施者に資力がなければ、情報持ち出し事案への対応に要した費用を回収することは現実的ではありません。

- ① 2014年に発覚した、ベネッセコーポレーションの顧客情報持ち出し事案：東京高裁において懲役2年6月（実刑）及び罰金300万円の判決。
- ② 2020年に発覚した、ソフトバンクから楽天モバイルへの転職者の技術情報持ち出し事案：東京地裁において懲役2年（執行猶予4年）及び罰金100万円の判決。
- ③ 2023年に発覚した、NTT西日本の子会社からの顧客情報持ち出し事案：岡山地裁津山支部において懲役3年（執行猶予4年）及び罰金100万円の判決。

3 企業が刑事事件化する理由、刑事事件化を希望する際の留意点

上記のとおり、費用回収等に関するメリットも少ない中、なぜ企業が刑事事件化するのか^[7]等、危機管理の観点から考えてみたいと思います。

（1）企業が刑事事件化する理由

ア 被害状況の把握

被害企業が刑事事件化する理由の1つとして、被害状況の把握・社内調査との照合が挙げられます。近年の情報持ち出し事案は、電子データをコピーして持ち出す方法のものが多くありますが、被害企業が専門業者に対して、デジタルフォレンジック調査（PC等のログ等のデータを保全し、それを分析する調査）を依頼することにより、「いつ、どのようなデータをコピーして持ち出したか」を一定程度調べることは可能です。しかし長期間・複数回にわたって持ち出しがなされているケース等では、これら被害状況の把握にも限界があります。

⁶ 経済産業省「営業秘密管理指針」（令和7年3月31日最終改訂）
（<https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/r7ts.pdf>）

⁷ 法21条7項のとおり、不正競争防止法違反は基本的に非親告罪（告訴がなくても刑事裁判を行うことができる罪）となっていますが、実務上は被害を受けた会社による告訴や捜査協力が求められます。

一方、捜査機関は、強制的な操作権限を元に、持ち出し行為の被疑者が個人的に所有するPCや契約しているサーバーの中身も調査する余地があり、これらに保存されているデータの分析によって、情報の持ち出し時期・範囲の全容が解明されることもあります。

捜査機関が強制的に被疑者の個人的なPCやサーバーの中身の調査をするためには、裁判所による令状の発布との関係でも相応の嫌疑の存在が必要となることから、社内調査を先行させ、その調査結果を捜査機関に申告する（また保全したPC等のデータも提供する）ことが効果的です。

こうした捜査の結果、公判（刑事裁判）に至った場合、検察官の陳述内容や提出証拠から被害状況を把握できる可能性があります。①被害企業として検察官に公判期日を確認して公判を傍聴する、②いわゆる犯罪被害者保護法により証拠を閲覧・謄写を請求する、③不起訴記録についても法務省の運用方針^[8]に従い閲覧・謄写を請求するといったことにより、被害状況の把握・社内調査の結果との照合を進めることができる余地が生まれます。

イ 開示先の牽制

被害企業としては、「いつ、どのようなデータをコピーして持ち出したか」の把握以外に、情報の持ち出し先企業（開示先）も把握して、それら情報を利用しないよう牽制・警告したいところです。しかし、情報持ち出しの被疑者の（同業の）転職先のように、疑わしい持ち出し先が明らかな場合を除き、開示先の把握は容易ではありません。

しかし、先ほど1（2）で述べたとおり、転得した者も刑事責任を負う場合があることも踏まえ、開示先にも搜索・差押え等の捜査がなされることもあり、かかる捜査が開示先の情報利用に対する牽制になることもあります。

（2）刑事事件化を希望する際の留意点

公判では検察官が営業秘密該当性を含む、不正競争防止法違反の被疑事実を主張立証することになりますが、その前段階として被害企業は捜査機関に協力することになります。しかし、営業秘密該当性、特に秘密管理性の主張立証に難がある状況では、公判に至る可能性は低くなってしまいます。被害が発覚してから、犯行当時の秘密管理性を主張立証しようとしても、適切な証拠（資料）が見つからない（失われている）ケースもありますから、平時から秘密管理性の確保及び管理状況を示す資料の保管には留意する必要があります。

また、繰り返し情報が持ち出された場合等が典型例ですが、検察官は全ての持ち出し行為を網羅的に起訴するとは限りません。したがって、公判での検察官の陳述、証拠、判決等から全ての持ち出し行為の時期、範囲を把握できるとは限りません。また、不起訴となった部分については記録の閲覧・謄写が許容される範囲も限られる（法務省側に裁量が大きい）ことから、捜査機関が動けば、情報持ち出しの全容が全て判明するとは限らない点には注意が必要です。

以上のような留意点、制約はあるものの、情報の持ち出し被害にあった企業としては刑事

⁸ https://www.moj.go.jp/keiji1/keiji_keiji23.html

事件の手続を通じて得られる情報も意識しつつ調査を進めていくことが有益であると考えます。

【執筆者】



齋藤 弘樹（弁護士）

E-mail: hiroki.saito@iwatagodo.com

2010 年東京大学法学部卒業

2012 年東京大学法科大学院 修了

2013 年弁護士登録

危機管理業務（平時の内部統制システムの整備や有事対応）と IT 関連業務を中心に手掛けている。

2 つの業務が交差する分野であるサイバー攻撃、情報漏えい、システム障害等に対する平時の体制整備・有事対応（官庁対応・顧客含む）を得意とする。

岩田合同法律事務所

1902 年(明治 35 年)、司法大臣や日本弁護士連合会会長を歴任した故・岩田宙造弁護士が「岩田宙造法律事務所」を開設したことに始まる、我が国において最も歴史のある法律事務所の一つです。開設当初より、我が国を代表する企業等の法律顧問として多数の企業法務案件に関与しております。日本法弁護士約 120 名が東京・札幌の両オフィスに所属し、日本語対応も可能な中国法弁護士、フランス法弁護士、米国各州弁護士資格を有する多数の弁護士のほか、特別招聘顧問として元最高裁判所長官大谷直人氏、特別顧問として前公正取引委員会委員長古谷一之氏、前金融庁長官井藤英樹氏が在籍しております。

〒100-6315 千代田区丸の内二丁目 4 番 1 号 丸の内ビルディング 15 階

岩田合同法律事務所 広報： newsmail@iwatagodo.com

※本ニュースレターは一般的な情報提供を目的としたものであり、法的アドバイスではありません。また、その性質上、法令の条文や出展を意図的に省略している場合があります、また情報としての網羅性を保証するものではありません。個別具体的な案件については、必ず弁護士にご相談ください。