

我が国における 技術流出及び管理の実態について

経済産業省知的財産政策室長
中原 裕彦

従業員による営業秘密の流出、国外への流出

具体的な事例

- 外国企業とのJVで開発していた触媒の作り方について、ノウハウを身につけた従業員が退職し、秘密保持契約に反して転職先でノウハウを漏らした疑いがある。
- 月曜朝の開空国際線到着ロビーで、当社の従業員が帰国したところを目撃した。アルバイトで外国の競合企業に技術指導に行っているのではないか。
- 日本国内に生産拠点を持たない外国企業が東京近郊に「デザインセンター」を設置し、リストラで早期退職した社員を大量に雇用している。毎日出勤する必要はないらしいが、2年たつてノウハウを吸い取ったら解雇されると聞く。
- コンピュータの周辺機器の販売担当部長が退職時に部下を引き抜くとともに、退職直前にメインフレームの稼働リストをプリントアウトして持ち出した。
- 生産部門の責任者である事業部長が外国企業に移籍し、その部下数名も移籍。その後の外国企業の開発・実用化のスピードをみるに、この元部長らが退職時に営業秘密が記録されたデータ等を持ち出したとしか考えられない。



技術流出事例① 設計情報13万件の持ち出し事件

中国人技術者による13万件の設計情報のダウンロードが発覚



貸与PCを自宅に持ち帰っていたこともあり、
中国人技術者宅を訪問し、貸与PC及び個人PCの提出を求めた。



貸与PCはデータが消去されたものが提出、
個人PCはハードディスクが壊されていた。

・会社から貸与PCの持出が可能であった。

・貸与PCは、インターネットメール、USBメモリとのアクセスログが判明したものの、どのようなデータのやりとりがされたかはわからなかった。

・個人用PCは、ハードディスクが壊されていたため、保存データの解析ができなかった。



中国人技術者は、事情聴取に応じず中国へ帰国。
日本に戻ってきた際に事情聴取するも、勉強目的であったなどの証言。

・証言からは不正目的が判明しなかった。



愛知県警がパソコン横領の罪で逮捕。
最終的には起訴猶予処分。

・不正競争防止法に該当するような、不正の競争の目的の存在、データを持ち出した物的証拠などが得られなかった。

技術流出事例② ロシアへの先端部品の流出事件

展示会に先端部品を出展した際に、説明者であった技術者が
在日ロシア通商代表部職員であったロシア人から声をかけられた。

・展示会がターゲットにされるケースもある。



交流を深め、論文などの提供を行っていたところ、
ロシア人からの要求は、次第にエスカレートしていった。

・飲食代などの提供を受けていたこともあり、断り難い状況になっていた。



技術者は別のロシア人への半導体部品提供事件が発生した後、
ロシア人との交流を中止するとともに、退社した。



警視庁の調査が行われ、窃盗容疑で書類送検されることとなった。
ロシア人への協力の動機として技術者は「自分の研究成果への職場の評価に不満があった」といった証言があった。



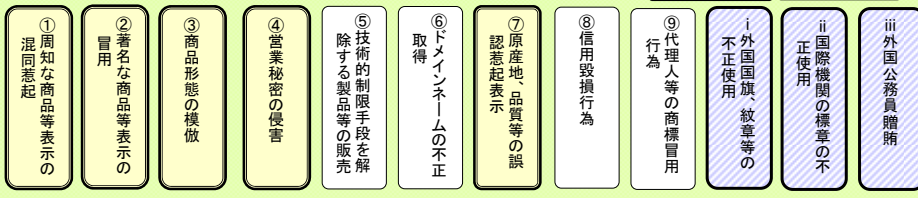
ロシア人は出頭要請に応じず帰国。
技術者においては、起訴猶予処分となった。

不正競争防止法の概要

目的

事業者間の公正な競争及びこれに関する国際約束の的確な実施を確保するため、不正競争の防止及び不正競争に係る損害賠償に関する措置等を講じ、もって国民経済の健全な発展に寄与する。

不正競争行為等の定義



措置の内容

刑事的措置

不正競争のうち、一定の行為を行った者に対して、以下の処罰を規定。

- 罰則(21条)
 - 第1項; 営業秘密侵害罪: 10年以下の懲役又は1000万円以下の罰金(併科可)
 - 第2項; その他の侵害罪: 5年以下の懲役又は500万円以下の罰金(併科可)
- 法人処罰(22条)
 - 営業秘密侵害罪の一部とその他の侵害罪の全部
 - 3億円以下の罰金
- 国外での行為に対する処罰(21条4項・5項・6項)
 - (営業秘密侵害罪、外国公務員贈賄罪)

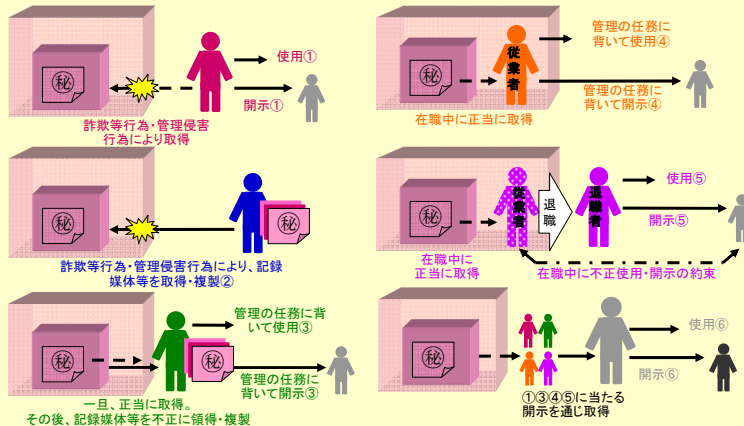
民事的措置

- 差止請求権(3条)
- 損害賠償請求権(4条)
- 損害額の推定等(5条等)
- 書類提出命令(7条)
- 営業秘密の民事訴訟上の保護(10条等)
 - (秘密保持命令、訴訟記録の閲覧制限、非公開審理)
- 信用回復の措置(14条)

営業秘密の刑事的保護①

- ▶ 営業秘密の不正な取得・使用・開示行為のうち、悪質な行為は、刑事罰の対象
- ▶ 国外犯(日本国内で管理されている営業秘密を海外で使用・開示する行為)も、刑事罰の対象
- ▶ 行為者のみでなくその者が所属する法人も処罰の対象

罰則の類型



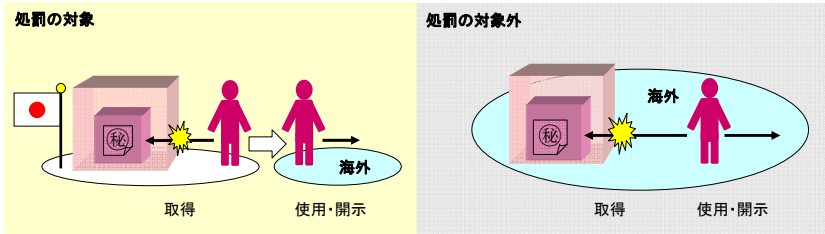
※○囲いの数字は、不正競争防止法第21条第1項各号の「罰則」に該当することを意味する。

詐欺等行為=詐欺、暴行、脅迫 管理侵害行為=媒体の窃取、施設への侵入、不正アクセス行為等

営業秘密の刑事的保護②

国外犯

- ◆ 詐欺等行為又は管理侵害行為が行われた際に日本国内で管理されていた営業秘密
 - ◆ 営業秘密の保有者から正当に示された際に日本国内で管理されていた営業秘密
- ⇒これらについては、**日本国外**で不正使用・開示行為が行われた場合についても、処罰の対象



罰則

10年以下の懲役又は1000万円以下の罰金。懲役刑と罰金刑を併せて科されることがあります。

法人処罰

法人の業務に関して前ページの①、②、⑥の犯罪が行われた場合には、行為者とともに、その者が所属する法人も処罰(3億円以下の罰金)の対象となります。

営業秘密管理指針(平成17年10月改訂版)

営業秘密の管理の意義

- 自社にとって大事な情報を、大切に保護すること
- 自社の従業員が、他社の営業秘密を侵害しないこと
- いずれも、企業と従業員とが共通の意識を持って取り組むこと

営業秘密の3要件

- 秘密管理性
- 有用性
- 非公知性

営業秘密を保護するための管理のあり方

- 民事判例を基に、不正競争防止法による保護を受けるために最低限満たすことが必要と考えられる「ミニマムの水準」を提示
- より実効性の高い管理水準として「望ましい水準」を提示。具体策について企業の実務とのすり合わせが重要



- 営業秘密の不正な取得・使用・開示行為に対し、差止め、損害賠償、信用回復措置の請求が可能

営業秘密の民事的保護

営業秘密の刑事的保護

- 営業秘密の不正な取得・使用・開示行為のうち、悪質な行為は、刑事罰の対象
- 国外犯も、刑事罰の対象
- 行為者のみでなくその者が所属する法人も処罰の対象

今後の検討の方向性(1)

「技術情報の適正な管理の在り方に関する研究会」

- ◆ 産業情報の流出は、海外展開に伴う現地への技術指導、特許情報へのアクセス等合法的なものから、外部からのハッキング、従業員の背信的な漏洩行為等の違法なものまで、多様な形態で生じる。
- ◆ 我が国は情報流出・危機管理に無防備であるという批判があり、近隣諸国は、我が国に係る重要情報のほとんどを、公開情報から得ているとの指摘がある。
また、違法な流出に対応するため創設された不正競争防止法の営業秘密侵害罪で実際に起訴された例はなく、その実効性の検証の必要性が指摘されている。
- ◆ こうした事態に対処するため、情報流出の全体像を鳥瞰し、法制度の在り方の検討等のハード的対応策から、企業の自主的取組の推進等のソフト的対応策まで、産業情報の適切な管理のための諸方策を総合的に検討するものとする。

今後の検討の方向性(2)

「技術情報の適正な管理の在り方に関する研究会」における検討内容

- ◆ 「流出を防止すべき情報」、「流出の経路」、「失われる保護法益」についての包括的な分析・整理
- ◆ 安全保障の視点
- ◆ 情報保全とイノベーションの視点
- ◆ 企業における情報管理
- ◆ 大学・研究所における情報管理
- ◆ 政府における情報管理
- ◆ カウンター・インテリジェンス体制の整備

今後の検討の方向性(3)

「情報」の「非移転性」以外の着目すべき特殊な属性

- ◆ 財産を生み出すポテンシャルを有していること(根源性)
- ◆ 一旦侵害されてしまうと、侵害者の下にその情報は留まり、また、侵害者の下に留まった状態において、さらに瞬時に拡散してしまうことが考えられ、秘密状態の回復が困難又は不可能であるという性質を有していること(不可逆性)
- ◆ 人的・組織的に十全の努力を尽くしてもなお、管理・予防し得ない性質を有していること(予防の困難性)