

経済産業省委託事業

タイにおける営業秘密管理マニュアル

2021 年 3 月

独立行政法人 日本貿易振興機構

バンコク事務所

(知的財産権部)

報告書の利用についての注意・免責事項

本報告書は、日本貿易振興機構（ジェトロ）が現地調査会社に委託し作成したものであり、調査後の法律改正などによって情報が変わる場合があります。掲載した情報・コメントは調査委託先の判断によるものであり、情報の正確性や一般的な解釈がこのとおりであることを保証するものではありません。また、本報告書はあくまでも参考情報の提供を目的としており、法的助言を構成するものではなく、法的助言として依拠すべきものではありません。本報告書にてご提供する情報等に基づいて行為をされる場合には、必ず個別の事案に沿った具体的な法的助言を別途お求め下さい。

ジェトロおよび調査委託先は、本報告書の記載内容に関して生じた直接的、間接的、派生的、特別の、付随的、あるいは懲罰的な損害および利益の喪失について、それが契約、不法行為、無過失責任、あるいはその他の原因に基づき生じたかにかかわらず、一切の責任を負いません。これは、たとえジェトロまたは調査委託先が係る損害等の可能性を知らされていても同様とします。

目次

はじめに	4
第1章 法制度編	6
1 タイにおける営業秘密の定義	6
2 営業秘密の管理方法	11
3 営業秘密の侵害行為	15
4 営業秘密侵害に対する法的保護	17
5 営業秘密に関する紛争事件の統計情報	25
6 最近の裁判例動向	26
第2章 漏えい対策実践編	40
1 タイにおける営業秘密管理の3ステップ	40
2 関連契約書作成上の留意点	49
3 漏えい事案への対応	51
第3章 各種関連書類参考書式（フォーム）	53
1 雇用契約における一般的な守秘義務条項例	53
2 従業員と締結する営業秘密に関する秘密保持契約の条項例	54
3 取引先等第三者と締結する営業秘密に関する秘密保持契約条項例	56

はじめに

本マニュアルは、タイにおいて事業を行う日系企業が、自社の技術やノウハウを保護するための施策を行う際の一助となるよう、営業秘密保護に関するタイの法制度と実務上の対応策を概説するものである。

本マニュアルは、大きく三部から構成されており、第1章においては2015年営業秘密法を中心にタイにおける営業秘密の保護にかかる法制度の概要を説明している。これを踏まえて第2章では、企業が実際にどのような対応をとるべきかについて、漏えいを防止するための平時の対応（社内ルールの策定と運用、関連当事者との秘密保持契約の締結等）と、情報が漏えいしてしまった場合における有事の対応（原因の究明と情報拡散の防止、法的措置の行使等）について解説する。また、社内規程の策定・拡充や社内外での契約締結の際の条項案として役立てていただけるよう、第3章では各種関連書類のサンプルを紹介している。

現代社会における情報技術の発達と、多様な情報関連サービスの発展によって、企業が事業活動において収集し、創出し、共有する情報の量は飛躍的に増大している。とりわけ、グローバルに事業を展開する企業においては、世界各国に点在する拠点が、製品やサービスに関する情報を瞬時に連携できることのメリットは計り知れない。その一方で、重要な企業秘密が盗用されるリスクや、一度漏えいしてしまった情報が拡散してしまうリスクも、かつてないほどに高まっていることに考えを巡らせなければならない。情報は最も弱いところから漏えいする。日本の本社においていかに堅牢な情報保護措置をとっていたとしても、海外の一拠点であったとしても保護の不十分な場所があれば、その一か所から情報は漏れ出てしまうのである。重要な企業秘密が、世界各国の拠点に共有されているのであれば、すべての拠点において十分な保護措置をとらなければならないのである。人的にも資金的にもリソースが不足した海外拠点が、情報保護のボトルネックとなってしまうような例が散見されるが、むしろ日本の本社から目の届きにくい海外拠点においてこそ、企業が秘密として管理しておく必要があるさまざまな情報の情報管理について、一層の注意を払わなければならない。

日本とタイとで法制度の違いはあるものの、営業秘密に対する基本的な考え方や対応策は共通するところも多い。したがって、日本において営業秘密保護の体制が整っている場合には、日本における規程や契約、具体的な管理体制・枠組みなどを参照しつつ、タイでの情報管理体制を整備する方法が有効である。もちろん、日本本社で使用している規程や契約等を、そのままタイ法人にも持ち込めばよいというものでもないが、特に日本とタイとで同種の事業や情報を扱う場合には、そのような対応が効率的であろう。本マニュアルでは、日本とタイとの営業秘密保護制度の差異についても言及しており、日本の本社での情報管理体制をタイ法人に対して応用するといった場合においても、役立てることができるものとなっている。

本マニュアルが、タイで事業を行う日系企業の営業秘密保護のために、何らか役立つ

ものとなれば幸いである。

第1章 法制度編

1 タイにおける営業秘密の定義

(1) 営業秘密を規律する法律

タイにおいて営業秘密の保護を規律する法律は、2015 年営業秘密法（Trade Secret Act B.E.2558、以下「営業秘密法」、「本法」、または「法」という。）である。本法は、2002 年に制定されていた営業秘密法（以下「2002 年法」という。）を改正して成立した法律である。日本においては営業秘密の保護が、不正競争防止法上の不正競争の一類型として規律されているのに対して、タイでは営業秘密を保護するための独立の法律が制定されている。

また、2002 年法のもとで、農薬製品及び医薬品について、営業秘密の保護を当局に求めるための、登録手続きを定めた規則が存在する。これらの規則は、農薬製品や医薬品の登録申請のために当局に提出する情報について、当局の担当官が登録された情報を一定期間、適切に保護することを義務付ける趣旨で定められているものである。これらの規則は現在も有効であるものの、登録それ自体が営業秘密と認められるための要件ではないため、実務上はほとんど利用されていない。

（営業秘密の登録手続きに関する規則）

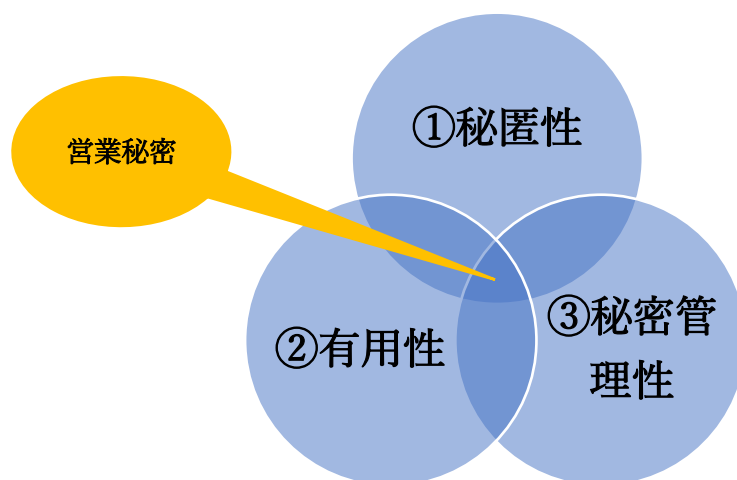
ア 農薬製品の登録に関連する規則

- ・ 農薬製品に関する営業秘密保護にかかる農業省規則 (B.E.2547)
- ・ 農薬製品に関する営業秘密の通知におけるガイドライン、方法及び条件にかかる農業省規則(B.E. 2547)

イ 医薬品の登録に関連する規則

- ・ 医薬品情報に関する営業秘密の維持にかかる公衆衛生省規則(B.E.2550)

(2) 営業秘密の 3 要件



法 3 条は、営業秘密の定義について、「営業秘密とは、未だ一般に公表されていない営業情報¹、または営業情報に通常触れることのできる者が、未だアクセスすることのできない情報をいう。ただし、当該情報が秘密であることによって商業的価値がもたらされ、当該情報の管理者が秘密を保持するために適切な手段を講じていなければならない。」と規定している。この定義を各要素に分解すると、以下の 3 要件として整理することができる。

表：営業秘密の 3 要件

No.	要件	内容
①	秘匿性	未だ一般に公表されていない営業情報、または営業情報に通常触れることのできる者が、未だアクセスすることのできない営業情報であること
②	有用性	当該情報が秘密であることによって商業的価値がもたらされること
③	秘密管理性	当該情報の管理者が秘密を保持するために適切な手段を講じていること

ア 秘匿性

上記要件のうち、要件①「秘匿性」とは、「当該情報が一般に公表されていないこと、または入手できる状況になっていないこと」を指す。当該情報が「営業情報」であることが求められているものの、営業情報とは広く情報を伝達する媒体を指しており、当該情報の営業的性質や商業性が求められているわけではない（こういった性質はむしろ要件②「有用性」の中で判断される）。

後記裁判例 No. 1-5(CIPITC, TorPor. 91/2563)においては、検索エンジンにおいて公表されている店舗関連情報（具体的には Google 社が提供するサービス「Google マップ」等に表示される店舗に関する情報で、店舗名、事業分類、営業時間等に関する情報）について、秘匿性を否定している。

イ 有用性

要件②「有用性」とは、「秘密が保たれることによって商業的価値があること」をいう。

前記「ア 秘匿性」でも言及した後記裁判例 No. 1-5(CIPITC, TorPor. 91/2563)は、検索エンジンにおいて公表されている店舗関連情報について、秘匿性のみならず有用性も否定している。そのような店舗関連情報は、秘密が保たれることではなく、むしろ公開されることによって価値を有する情報だからである。

¹ 「営業情報」とは、「伝達方法及び伝達形態にかかわらず、趣旨、内容、事実、またはその他の意味を伝える媒体を指し、調整法、様式、解釈、もしくは結合したもの、プログラム、方法、技術、または工程を含む」と定義されている（法 3 条）。

有用性の要件は、当該情報を秘密に保つことによってもたらされる価値があるかどうかという、実質的な要件として機能している（したがって、後記「(3)日本における営業秘密との異同」において述べるように、日本における有用性の要件よりも広い概念である）。

ウ 秘密管理性

要件③「秘密管理性」とは、「当該情報を秘密に保つための措置が行われていること」を意味する。営業秘密をめぐる裁判例において、最も紛争になりやすい争点である。上述の要件①及び要件②が情報の性質そのものに着目した要件であるのに対して、本要件③は営業秘密を保有している企業における情報管理の方法と体制が十分であるか否かが問われていることから、営業秘密管理体制の構築にあたっては、特に本要件③が認められるのに十分な秘密管理措置を確保できているかという視点を持たなければならない。また、社内規程や就業規則において秘密保持に関するルールを定めるのみでは足りず、当該情報が秘密に保たれるための運用が実際に行われている必要がある。いかに精緻なルールが制定され、従業員にルールを守る義務が課されていても、そのルールや義務が実際に運用されず形骸化されているのでは、秘密を保つための措置が行われているとはいえないのである。これに加えて、社内教育や監査を通じて、実運用においても営業秘密の管理が徹底されていなければならない。

例えば、後記裁判例 No.2-2 (最高裁判所 No. 19015/2555)において、就業規則において従業員に対して一般的な秘密保持義務を課すのみでは秘密保持措置として足りないことが述べられている。

具体的な営業秘密管理措置としては、後記裁判例 No.1-3 (特別専門事件控訴裁判所, No. 732/2560、CIPITC, TorPor. 8/2560)において以下のような要素が言及されている。

- (ア) 営業秘密となる情報を特定し、維持するための内部規則を制定し、実施すること
- (イ) 文書を機密情報としてマークすること
- (ウ) 従業員が会社の秘密を漏らさないよう契約を締結すること

具体的な営業秘密管理措置としては後記 2(1)及び(2)のとおり、会社が営業秘密として指定した情報について、アクセス制限、パスワードの付与、施錠可能なキャビネットにおける保管といった措置をとることが重要になる。

なお、後記裁判例 No.1-1 (CIPITC, TorPor. 104/2563) でも言及されているように、秘密管理措置の程度は、情報の保有者と同じ立場、状況にある合理的な者の基準に照らして、適切な措置をとることで足りる。したがって、秘密管理措置が十分であるか否かについて絶対的な基準が設けられているのではなく、

企業の実態や規模等の事情に照らして、相対的に判断される。

(3) 日本における営業秘密との異同

日本においては、不正競争防止法において営業秘密の保護が規定されており、営業秘密とは「秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上または営業上の情報であって、公然と知られていないものをいう」と定義されている（同法2条6項）。すなわち、日本においても営業秘密の要件は3要素からなっており、保護を受ける上で営業秘密として認められるためには、①秘密管理性（秘密として管理されていること）、②有用性（事業活動に有用な技術上または営業上の情報であること）、③非公知性（公然と知られていないものであること）を満たす必要がある。

日本とタイにおける営業秘密の異同を表にまとめると以下のようになる。

表（日本とタイにおける営業秘密の異同）

	日本	タイ
1. 法律	不正競争防止法	営業秘密法
2. 営業秘密の定義	秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上または営業上の情報であって、公然と知られていないもの（2条6項）	未だ一般に公表されていない営業情報 ² 、または営業情報に通常触れることのできる者が、未だアクセスすることのできない情報をいう。ただし、当該情報が秘密であることによって商業的価値がもたらされ、当該情報の管理者が秘密を保持するために適切な手段を講じていなければならない（3条）
3. 営業秘密の要件	①非公知性 ②有用性 ③秘密管理性	①秘匿性 ②有用性 ③秘密管理性

上述のとおり、日本とタイにおける営業秘密の定義及び要素がきわめて類似していることが分かる。これは、WTO（世界貿易機関）の TRIPS 協定（知的所有権の貿易関連の側面に関する協定）のもとで、WTO 加盟国は同協定の「開示されていない情報」に

² 前掲脚注1参照。

関する規定にもとづいて営業秘密保護を国内法に反映させる義務があり、日本もタイも、同規定に適合する法制度を導入しているためである。同協定においては、以下の(a)から(c)に該当する開示されてない情報について、公正な商慣習に反する方法により、自己の承諾を得ずに、他者が情報を開示、取得、または使用することを防止できるような保護を与えなければならないとされている（TRIPS 協定 39 条 1）。

- (a) 当該情報が一体としてまたはその構成要素の正確な配列及び組立てとして、当該情報に類する情報を通常扱う集団に属する者に一般的に知られておらずまたは容易に知ることができないという意味において秘密であること
- (b) 秘密であることにより商業的価値があること
- (c) 当該情報を合法的に管理する者により、当該情報を秘密として保持するための、状況に応じた合理的な措置がとられていること

(a)が秘匿性または非公知性、(b)が有用性、(c)が秘密管理性にそれぞれ対応しており、この要件をもとに日本及びタイの営業秘密の要件が構成されている。

もっとも、日本及びタイにおいて、営業秘密の要件自体は共通していても、その要件が裁判において認められるための水準には、差がある。たとえば日本においては、営業秘密の要件のうち「有用性」の要件を満たさないと判断されることは少なく、原則として事業活動に有用な技術上または営業上の情報であれば一般に有用性の要件を満たすとされている。有用性の要件が否定されるのは、公序良俗違反や反社会的な情報に限定されると解されているのである。この点、タイにおいては当該情報が秘密に保たれることによる価値があるか否かを実質的に考慮するなど、有用性の判断基準が異なる水準で適用されている。タイにおける個々の裁判例での営業秘密性の判断については、本章 6 「営業秘密法の改正及び最近の裁判例動向」において述べる。

(コラム) 営業秘密保護と個人情報保護の関係性

企業が保護すべき情報として、営業秘密の他に個人情報がある。タイにおいては長らく個人情報保護を包括的に規律する法律が定められておらず、個人情報の漏えい等に対しては民商法上の不法行為の枠組みの中でのみ救済が可能であると考えられていた。個人情報の取得、利用、開示を行うにあたって本人の同意を得るといったルールも特段定められていなかった。

2016 年に欧州において一般データ保護規則（General Data Protection Regulation、以下「GDPR」という）が制定されたことをきっかけとして、世界的にパーソナルデータ保護の意識が高まる中で、タイにおいても 2019 年 5 月に個人情報保護法（Personal Data Protection Act B.E.2562、以下「PDPA」という）が制定された。PDPA は、GDPR をベースに起草されたといわれており、事業者には厳格な個人情報保護法の義務が課される。本来は、成立から 1 年間の猶予期間を経て、2020 年 5 月から民間事業者への適用が開

始される予定であったが、2019年末から世界的に流行した新型コロナウイルス(COVID-19)の影響を受けて民間事業者の準備態勢が整っていないなどとして、適用開始がさらに1年間延期され、2021年6月から適用開始となることが予定されている。

PDPAの適用開始後においては、営業秘密の管理のみならず、個人情報の管理にも留意する必要がある。B to C事業者の場合であれば、消費者情報の管理体制を見直す必要があるほか、B to B事業者の場合には従業員の個人情報保護を中心に情報管理体制の整備を進める必要があるだろう。場合によっては、消費者や従業員本人から個人情報の取扱いに関する同意書を取得する必要があるほか、会社ウェブサイト等において法定の通知事項を網羅したプライバシーポリシーを掲示する必要もあろう。

営業秘密保護と個人情報保護は、いずれも情報の流出・流通の防止に向けてアクセス権限の管理といったセキュリティ上の対策においては共通するところが多いものの、その制度趣旨が異なるうえ(営業秘密保護はこれを保有する事業者の保護を目的としているが、個人情報保護はむしろ個人の自身に関する情報についての権利擁護を目的としている。)、秘密の対象となる情報に触れる従業員も異なることから、具体的な対応策や主たる管掌部署も異なることが多い。

これまで個人情報保護の法整備がなされていなかったタイにおいては、日本以上に、従業員の情報管理意識の向上につとめる必要がある。ひとたび情報漏えいが生じると、PDPA上の制裁を受ける可能性があるのみならず、ビジネスパートナーからの信頼を失ったり、SNS上での炎上事案につながったりといったレピュテーションリスクもある。タイで事業を行う日系企業においては、営業秘密管理体制の整備に加えて、個人情報保護についても意識を高め、消費者や従業員に対する権利侵害を起こさぬよう注意しなければならない。

2 営業秘密の管理方法

(1) 社内における営業秘密管理の留意点

ア 社内規程(営業秘密管理規程)の策定

上記1に述べた通り、ある情報が営業秘密と認められるためには、秘密管理性が認められなければならない。会社内であっても誰もが当該情報にアクセスできてしまうのでは、営業秘密性が認められない。たとえば、後記裁判例 No.1-6(最高裁判所, No. 1323/2560/ CIPITC, TorPor. 102/2557)においては、ある情報が、いずれの従業員でも開けることのできるキャビネットに保管され、誰でも知ることのできるパスワードを付してコンピュータに保存されていた事実を認定して秘密管理性を否定している。また、裁判例 No.2-2(最高裁判所, No. 19015/2555/ CITIPC, Or. 5035/2553)においては、ある情報が、屋外の製造現場において保管されており、すべての従業員がそこへアクセス可能であったとして、秘密管理性を否定している。業務上、当該情報にアクセスすることが必要な者

に対してのみ、会社はアクセス権を与えなければならない。営業秘密の管理体制構築にあたっては、単に情報を社外秘として会社内に留めるというのみでは足りず、さらに一步進んで、社内の誰（どの部署の、どのレベルの役職の者）に対して、情報へのアクセスを認めるのかという粒度での検討を行わなければならない。

また、どの情報を営業秘密として保護しなければならないかについても、あらかじめ検討を行い、ルールとして明確化する必要がある。会社内のあらゆる情報をすべからず保護すべしと定めるだけでは、結局のところ、どの情報も特別には保護をしていないと考えられてしまう。製品の技術にかかる情報、材料原価にかかる情報、顧客にかかる情報等、会社の事業内容に照らしてどの種類の情報を特に秘密に保たねばならないかを検討したうえで、情報を取扱う個々の従業員にとってそれが秘密情報であると認識できるようにしなければならない。

なお、この段階では、その情報が実際に裁判において営業秘密と認められる可能性が高いか否かを厳密に考える必要はない。営業秘密性の判断は個々の事案ごとに異なるし、法律上の営業秘密として認められないとしても、それと同一水準のルールを適用することで事実上の情報漏えいリスクを下げることができるためである。たとえば、秘匿性や有用性の観点から必ずしも法律上の営業秘密として認められない可能性が高い情報であっても、事業運営上、それが社外に漏れることが好ましくなく、競業他社や顧客に知られることを防ぎたいと考える場合には、少なくとも社内ルール上は営業秘密又はそれに準じた保護対象として扱ってよい。

営業秘密として管理する情報の類型と、その情報へのアクセス権者を定めるルールとして、営業秘密管理規程といった社内規程を定めることが一般的である。

イ 物理的、技術的安全管理措置の策定

社内規程においては、情報の類型とアクセス権者のみでなく、具体的な秘密管理の方法も定めることとなる。具体的には、一定の種類の情報については、以下のような対応をとることが考えられる。

- ・物理的な情報遮断としてロッカーに鍵をかけて保管する
- ・当該情報のある部屋への入退室管理を実施する
- ・印刷物に「秘密」または「厳秘」といったスタンプを押す
- ・取締役会や会議で配布した資料はその場で回収、廃棄する

また、技術的な情報遮断措置としては、以下のような方法がある。

- ・社員アカウントごとのアクセス制限をかける
- ・ファイルにパスワードを設けてパスワードを知っている者だけがファイル

にアクセスできるようにする

ウ 安全管理措置の定め方

秘密管理の方法を定めるうえで注意すべきは、秘密の管理を厳重にすればするほど、当該情報の使い勝手は悪くなるということである。たとえば、ごく日常的に使用する製品図面を、常に鍵のかかるロッカーで保存し、権限のある者の決裁を得なければ取り出すことができないというのでは、秘密管理の方法としては厳重かもしれないが、日常業務に支障をきたしてしまう。そして、当該情報の利用頻度に比して不均衡なまでに厳重な秘密管理方法は、結果としてルールの形骸化を生み、策定されたルールと実務運用との間に乖離が生じる結果、営業秘密としての情報管理が行われなくなってしまう可能性がある。先の例でいえば、書類を使うために毎回上長の決裁を得るのは面倒だから、一度図面を借りたらしばらく持ったままでいよう、自分のデスクに置いておこうということになりかねない。あるいは、原本の管理が厳重なので、コピーを手元に置いておこうということにもなりかねない。過度に厳格なルールはかえって形骸化してしまうだけであるから、実際の業務運営に照らして実務上機能するようなルール作りをしなければならない。そのためには、情報管理のルールを一方的に作って守らせるという姿勢（あるいは日本本社が策定したルールをそのまま適用するという対応）ではなく、当該情報を扱う現場のスタッフにも情報管理の重要性を理解してもらったうえで、実行可能なルール作りに協力してもらうことが重要である。社内ルールの策定方法については、第2章「漏えい対策実践編」において詳しく述べる。

なお、秘密管理措置を実施する際の水準として、後記裁判例 No.1-1（CIPITC, TorPor. 104/2563）は、当該情報の保有者と同じ立場、状況にある合理的な者の基準に照らして、適切な措置でなければならないことを判示している。すなわち、秘匿したい情報の性質によって、秘密管理措置の強弱をつけることも可能と考えられる。同裁判例において具体的には、太陽光発電事業者が、太陽光発電候補地を検討するために行うデューデリジェンスの報告書は、性質上投資家への開示が予定されているものであるから、たとえば開発中の新薬や化合物の情報等に比すれば、厳格な秘密管理措置までは求められないとされている。この点、日本における秘密管理性の判断においても、秘密管理措置の絶対的な基準が定められているわけではなく、企業の実態や規模等の事情に応じた合理的な秘密管理措置で足りると解されていることと共通している。

(2) 社外に対する営業秘密管理の留意点

ひとたび社外に開示してしまった情報は、会社のルールや規制が及ばなくなるため、情報管理が一層難しくなる。営業秘密を社外に出すことは慎重にならなければ

ならない。具体的には、取引先等の社外の者に対して営業秘密を開示する場合には、常に当該情報の受領者との間で秘密保持契約（No Disclosure Agreement、以下「NDA」という）を締結すべきであり、NDA の締結までは相手方に営業秘密を開示してはならない。秘密保持義務を課さずに第三者に開示した情報については、営業秘密の要件のうち秘匿性や秘密管理性が失われてしまう可能性がある。なお、取引先と締結する NDA 文案については、第 3 章「各種関連書類参考書式（フォーム）」を参考にされたい。

社外への情報開示と類似の場面として、従業員の退職による情報漏えいのリスクがある。業務において営業秘密を取扱っていた従業員が退職してしまうと、当該従業員が競業他社に転職して営業秘密（技術情報や顧客情報）を持ち出してしまう可能性や、当該従業員自身が同種の事業を行う会社を立ち上げてしまう可能性がある。従業員の退職後は、社内ルールを守らせることや、就業規則違反に基づく懲戒処分とすることもできないから、雇用契約の秘密保持義務違反を退職後も一定期間課す方法や、退職時に NDA を締結する方法により、契約上の義務として情報保持義務を課さなければならないのである。また、営業秘密とは別に、実質的に競業他社への情報漏えいを防ぐ方法として、従業員に対して競業避止義務を課すことも考えられる。

（コラム）従業員の競業避止義務の有効性

従業員に対して退職後の競業避止義務を課すことは、タイにおいて一般に有効と考えられている。もっとも、いかなる競業避止義務であっても無制限に有効とされるのではなく、裁判所が不公正な契約内容であると判断した場合には、競業避止義務の一部期間について無効と判断される場合がある。具体的には、競業避止義務の対象となる事業の範囲と期間が、当該従業員が従事していた業務内容、役職、または支払われていた賃金に比して合理的な範囲内といえるか否かが総合的に考慮されるのである。なお、競業避止義務に対する経済補償金の支払いは、有効な競業避止義務を課すための要件とはされていない。あくまでも競業避止義務の合理性を検討する際の、一考慮要素として扱われるに留まる。

競業避止義務の有効性に関する判例として、最高裁判所, No.9276/2559 がある。同判決においては、会社が従業員（調達部門の副マネージャー）に対して「労働契約継続中及び終了後 24 か月間、ASEAN 地域において競業事業を経営し、または競業他社において勤務することを禁止する」とする内容の競業避止義務の有効性が争われた。同判決は、①当該従業員が会社において勤務した期間が 1 年 10 か月間に過ぎないこと、ならびに②会社が有する知識及び経験は当該従業員が当初から有していた経験に及ばないものであったことを考慮して、競業避止義務を 3 か月間に限り有効と判断した。

当該事案のように、競業避止義務の期間が過度に長期と判断される場合には、裁判所

によって一部期間について無効と判断されるリスクがある。もっとも、3 か月を超えれば一律無効になるという性質のものではなく、どの程度の競業避止義務期間であれば確実に有効であるということを、確実に予見することは難しいため、実務上は、競業避止義務期間の一部が将来の裁判において無効と判断されるリスクを踏まえても、ある程度長めの競業避止義務期間を設定しておく例も多い。

(3) 営業秘密の国外への持出しにかかる留意点

タイにおいては、営業秘密の国外持出しにかかる特段の規定は存在しない。一方で、2019 年 4 月 30 日に官報掲載された大量破壊兵器及び関連品目貿易管理法 (Trade Controls on Weapons of Mass Destruction Related Items Act、以下「TCWMD 法」という。) において、軍事用途に転用可能な物品の輸出管理規制が定められているが、当該法律に基づく関連法規が整備されていないため、実際には輸出管理規制が行われていない状況である。今後、関連法規が整備されると、この輸出管理規制の対象となる物品であって営業秘密情報が含まれるものの輸出に制限がかかる可能性はあるものの、現時点では TCWMD 法の規制なく物品の輸出が可能である。

(4) 登録の要否

営業秘密法上、営業秘密として認められるために登録を行うことは必要ない。

なお、農薬製品及び医薬品については、前記 1(1)のとおり当局に対して営業秘密保護を求めるための登録手続きを定めた規則が存在するものの、前述のとおり営業秘密として認められるための要件ではない。あくまでも、当局の担当官が登録された情報を一定期間、適切に保護することを義務付ける趣旨の制度であり、実務上ほとんど利用されていない。

3 営業秘密の侵害行為

(1) 営業秘密の侵害行為の種類

タイにおける営業秘密の典型的な侵害類型は、大別すると、以下のとおりである。

- ・従業員や元従業員が競合他社に対して会社の秘密情報を漏えい（販売）するケース（後記裁判例 No.1-1 (CIPITC, TorPor. 104/2563)、裁判例 No.1-3 (特別専門事件控訴裁判所, No. 732/2560/ CIPITC, TorPor. 8/2560)等)
- ・退職した元従業員が、会社の秘密情報（製造工程や顧客リスト）を利用して新会社を設立してしまうケース（後記裁判例 No.1-2 (最高裁判所, No. 7769/2557/ CIPITC, TorPor. 98/2551)、裁判例 No.2-1 (CIPITC, No. 5275/2549)等)

では、どのような要件を満たす行為が営業秘密の侵害行為にあたるのか。営業秘密法上、営業秘密侵害行為は「営業秘密保有者の許可なく、営業秘密を開示し、持出し、または使用する行為で、正当な商業手法に違反するものをいう。ただし、違

反者において、これらの行為が正当な商業手法に違反すると認識していたか、または認識するに足る根拠がなければならない。」とされる（法6条）。すなわち、営業秘密の侵害行為は、①侵害行為、②無許可、③非正当性、④非正当性の認識の4要件から構成される。

表：営業秘密侵害の4要件

No.	要件	内容
①	侵害行為	営業秘密を開示、持出しまたは使用
②	無許可	営業秘密保有者の許可を受けていないこと
③	非正当性	正当な商業手法に違反する行為であること
④	非正当性の認識	違反者において、当該行為が正当な商業手法に違反すると認識していたか、または認識するに足る根拠があること

このうち、③非正当性については、正当な商業手法に違反する行為であることというとされており、正当な商業手法に違反する行為としては、契約違反、秘密保持違反の侵害もしくは侵害するよう教唆する行為、贈収賄、脅迫、詐欺、窃盗、盗品の受領、または電子もしくはその他の方法を使った諜報行為が例示列举されている（法6条）。

この点、後記裁判例 No.1-4 (CIPITC, TorPor. 18/2563)において言及するように、会社が取扱う営業情報（不動産仲介事業者における不動産情報）を、営業担当の住宅アドバイザーが、会社のメールアカウントから個人のメールアカウントに送信することが、非正当性の要件を満たさないと判断した裁判例がある。したがって、会社の営業秘密を個人メールアカウントに送信することは、場合によっては、正当な商業手法に違反すると認定されない可能性がある。

従業員の私用メールアカウントにおいて営業秘密を利用させないためには、就業規則、雇用契約、秘密保持誓約書等により、会社の営業秘密を私用メールアカウント及び私用 SNS に送ってはいけない旨を明確に規定する必要があるだろう（SNS 利用の留意点については第2章 1(3)イ(イ)のコラム参照）。

(2) 侵害行為の例外

営業秘密侵害の例外として以下の4類型の行為が定められている。次のいずれかに該当する場合には、営業秘密侵害に該当しない（法7条）。

ア 営業秘密侵害の認識がないこと

営業秘密を取得した者が、他人の営業秘密を侵害して取得した情報であると認識せず、または認識するに足る根拠なしに、営業秘密を合法的に開示または使用すること

イ 政府機関による正当な開示または使用

政府機関が以下の（ア）または（イ）いずれかの場合において、営業秘密を開示または使用すること

（ア）公衆の衛生または公の秩序を保護するために必要な場合

（イ）商業目的でない公共の利益のために必要な場合であって、当該営業秘密を監督する政府機関、または当該営業秘密の取得に関係する政府機関もしくは関係者が不正な商業手法に使用されないよう、営業秘密保護のために合理的措置を講じて業務を遂行した場合

ウ 営業秘密に依拠しない独立の発見

自己の知識または専門にもとづき、他人の営業秘密を独自に発明または創出すること

エ リバース・エンジニアリング

一般に知られている製品の評価及び解析をすることによって、当該製品の発明、製造または開発手法を探索する目的で、他人の営業秘密を発見すること。ただし、評価及び解析をする者が、当該製品を善意で取得したのでなければならぬ。また、営業秘密保有者または製品の販売者との間でリバース・エンジニアリングを行わない契約を結んでいる場合はその限りではない。

4 営業秘密侵害に対する法的保護

(1) 裁判制度の概説

営業秘密に関する訴訟は、原則として知的財産権及び国際通商裁判所（いわゆる IPIT Court）が管轄権を有する（知的財産権及び国際通商裁判所の設置及び手続に関する法律 7 条 9 項、以下「IPITC 法」という。）。

IPITC 法上は、①中央知的財産権及び国際通商裁判所（The Central Intellectual Property and International Trade Court、以下「CIPITC」という）と、②地方知的財産権及び国際通商裁判所が設置されることとなっているものの、②は未だに設立されていない。したがって、本来であれば CIPITC の管轄権はバンコク、サムットプラカーン、サムットサコーン、ナコンパトム、ノンタブリー及びパトンタニ県の 6 県に対してのみ及ぶのであるが、現時点では CIPITC が全国の知的財産権に関する紛争について管轄を有している。

また、CIPITC における判決に不服がある者は、2016 年までは最高裁判所に対して直接上訴することとされていたが、2016 年以降は特別専門事件控訴裁判所に控訴することができ、さらに最高裁判所に上告することが可能となっている（2016 年特別専門事件控訴裁判所に関する勅令による。）。

なお、CIPITC 以外の裁判所でも営業秘密性が争われる可能性がある。たとえば、雇用契約に基づく権利義務に関する争いや雇用契約の遂行にかかる損害の請求は

労働裁判所が管轄権を有している。したがって、雇用契約違反に基づき労働裁判所に訴えを提起した場合で、当該契約違反の有無を争う中で、営業秘密侵害があったか否かが争点となるような場合がありうる。もっとも、請求の基礎として営業秘密侵害が主張される場合には、前記 IPITC 法 7 条 9 項に基づき CIPITC が管轄権を持つことから、営業秘密侵害を争う大半の訴訟は CIPITC に係属することとなる。以下(2)以下についても、CIPITC における紛争であることを前提として民事及び刑事における訴訟手続きの概要を述べる。

(2) 民事的措置（救済）

ア 救済の類型

営業秘密に対する侵害が現に行われ、または侵害がなされようとしていることについて、明らかな証拠がある場合には、営業秘密の管理者は以下（ア）及び（イ）の権利を有する。

(ア) 当該営業秘密権の侵害の仮の差止めを命ずるよう請求することができる。当該請求は（イ）における訴訟提起の前に行行使することができる。

(イ) 違反者による営業秘密の侵害を恒久的に禁止するよう求め、かつ違反者に対して損害賠償を請求することができる。

（ア）が仮差止め請求を、（イ）が差止め請求及び損害賠償請求を認めるものである。（イ）についてはさらに、営業秘密が公表されてしまった等の事情で差止めによる救済が適切でない特別な場合においては補償金の支払いを命ずることができること、営業秘密を侵害する材料、装置、道具、またはその他の設備についての破棄命令ができること、営業秘密の侵害によって製造された製品の所有権を国または営業秘密保有者に移転する命令ができる（法 11 条）。

営業秘密侵害に対する請求の時効は、営業秘密侵害とその侵害者を知ってから 3 年である。もっとも、侵害の日から 10 年を超えることはできない（法 10 条）。

イ 権利行使の主体

民事的救済の権利行使者は営業秘密の管理者である。これは前記 3(1)で述べた「営業秘密の保有者」よりも広い概念で、営業秘密の保有者に加えて、営業秘密の所持者、管理者、及び監督者を含む概念である（法 3 条）。

もっとも、営業秘密の所持者、管理者、及び監督者について具体的な定義は定められておらず、その範囲は必ずしも明確ではない。実際には裁判例のほとんどが営業秘密の保有者によって提起されている。

ウ 証拠収集

裁判所は、証拠が失われ、または提示が困難になる可能性がある場合には、証拠保全を命じることができる。また、緊急の場合には、証拠として用いられ

る資料の差押さえを命じることもできる（IPITC 法 28 条）。

エ 秘密保持のための手続き（非公開手続き及び秘密保持命令）

裁判所は、当事者の請求に基づき、審問の全部または一部について傍聴を禁止し、審問を非公開で実施すること、または事件における事実の公表の禁止を命じることができる（知的財産及び国際貿易事件のための規則 24 条）。

オ 立証責任（立証責任の軽減）

製品の製造過程についての営業秘密の管理者が、営業秘密の侵害を行った者に対して民事訴訟を提起する場合、侵害者が製造した製品が自己の営業秘密である製造過程を使用して製造された製品と同一であると証明できれば、侵害者が当該製品の製造に営業秘密を使用したと推定される（法 12 条）。

カ 損害賠償

裁判所が賠償金を定める場合、次に掲げる原則に従って決定することができる（法 13 条）。

(ア) 裁判所は、実際に発生した損害に対する賠償金を定めるだけでなく、営業秘密の侵害を行った者に対し、侵害によって直接的または間接的に得た利益を賠償金に加算して返還するよう命ずることができる

(イ) 上記（ア）に基づいて賠償金を定めることができない場合、裁判所が適当だと判断した金額の賠償金を定めることができる

(ウ) 営業秘密の侵害が、故意もしくは悪意に基づき秘密性を失わせる行為である明らかな証拠がある場合、裁判所は、（ア）または（イ）に基づいて定めた金額よりも高額 of 懲罰的賠償金を支払うよう命ずることができる。ただし、（ア）または（イ）に基づく金額の 2 倍を超えてはならない

(3) 刑事的措置（刑事罰）

ア 刑事犯の種類

本法は、営業秘密の侵害に対する犯罪類型として以下の罪を定めている。なお、いずれの下記犯罪類型についても未遂犯は可罰的である（刑法 80 条）。予備罪及び共謀罪の処罰規定は存在しない。

No.	類型	内容	親告罪
①	営業秘密侵害罪(33条)	営業秘密管理者が事業を営む上で損失を被るよう、悪意により他人が保有する当該営業秘密を営業秘密でなくなるよう、一般に認識されるよう公開した者には、文書、音声放送もしくは映像放送を使用した公開、またはその他の方法によって開示したかに関わらず、1 年以下の禁錮刑もしくは 20 万バーツ（約 70 万円）以下の罰金、またはその両方を科す。	親告罪

②	化学物質、農薬、化学製品の許可にかかる政府機関の営業秘密侵害罪（34条）	法 15 条 1 項の規定に基づき営業秘密を維持する立場にある者（化学物質、農薬、または化学製品の製造、輸入、輸出または販売許可のため政府に提出されたデータを保管する政府機関）が、営業秘密を不法に開示し、または自己もしくは他者の利益のために使用した者は、2 年以下の禁錮刑もしくは 10 万バーツ（約 35 万円）以下の罰金、またはその両方を科す。	非親告罪
③	本法上の義務に反する営業秘密侵害罪（35 条）	本法に定める義務の履行の過程で通常秘密に保たれるべき営業秘密管理者の事業に関連する事実を開示した者は、1 年以下の禁錮刑もしくは 10 万バーツ（約 35 万円）以下の罰金、またはその両方を科す。	非親告罪
④	両罰規定（36 条）	営業秘密の侵害を行った者が法人の場合には、当該法人における取締役、監督者、またはその他責任ある者としての指示、行為、不指示、不作為によって営業秘密を侵害した者に対しても同様の罰を科す	親告罪

②及び③については処罰対象が特に限定されている。すなわち、②の処罰対象は、前記 1(1)で述べた農業省及び公衆衛生省の規則により秘密情報を保持する義務が課された者である。また、③の処罰対象は本法に定める義務を有する者であるが、具体的には営業秘密侵害について捜査を行う警察官等を指す。したがって、②及び③は法律上の義務が特に課された者に課される刑事罰であり、一般的な刑事罰を定める規定は営業秘密侵害罪（33 条）である。同罪の構成要件は以下のとおりである。

- (ア) 営業秘密を公に開示したこと
- (イ) そのことにより秘密でなくなったこと
- (ウ) 事業を妨げる悪意があったこと（加害目的）

民事的措置において述べた、営業秘密の侵害行為と比較すると、刑事的措置では営業秘密の公表が要件に含まれているものの、営業秘密を特定少数の者に開示する場合は、本罪を構成しないと判示されている判例も存在するため、実態としては対象となる行為態様は著しく限定されている。

上記要件（ア）に関連して、過去の裁判例においては、飲食業チェーン店の食べ物や飲み物のレシピをウェブサイト上で公開したことにより、本罪の成立

を認めた例がある³。他方で、後記裁判例 No.2-1 (CIPITC, No. 5275/2549)は、会社の元従業員 5 名が独立して新会社を設立し、元働いていた会社の営業秘密を利用して事業を行ったという事案において、6 名（新しく設立された法人を含む）への営業秘密の開示は、公の開示にあたらないと判示した。

イ 訴追権者

なお、日本の刑事訴訟手続きにおいては、起訴独占主義のもとで刑事事件を起訴する権限は検察官のみに与えられているが、タイにおいては私人による訴追が認められている（刑事訴訟法 28 条）。また、検察官が起訴した事件の共同訴追者となることも認められている（刑事訴訟法 30 条）。

ウ 公訴時効期間及び告訴期間

営業秘密侵害罪の公訴時効期間は 5 年間である（刑法 95 条）。また、告訴期間は犯人を知った日から 3 か月間である（刑法 96 条）。

エ 秘密保持のための手続き

民事的措置の中で述べた、裁判手続きにおける秘密保持のための措置（前記 4(2)エ）は刑事訴訟の場合にも適用がある（知的財産及び国際貿易事件のための規則 42 条）。

オ タイ国外における営業秘密侵害罪について

刑事罰はタイ国外において行われた行為についても適用される場合がある（刑法 4 条、5 条）。典型的な場面としては、行為の一部がタイで行われた場合や、行為の結果がタイ国内で生じる場合が挙げられる。日系企業のタイ現地法人の営業秘密が、タイ国外で侵害された場合には、営業秘密侵害による損害（結果）が当該タイ現地法人において生じることから、営業秘密の開示行為自体が国外で行われたとしても、タイの営業秘密侵害罪が適用される場合があるものと考えられる。

（コラム）営業秘密法以外の刑事犯

本文において述べたとおり、営業秘密侵害に対して刑事的措置をとるにあたっては、「営業秘密を公に開示したこと」の要件が充足されなければならない点に大きな障壁がある。典型的な営業秘密侵害行為の場合、営業秘密を競業他社に開示する場合にせよ、営業秘密を利用して自ら会社を立ち上げる場合にせよ、当該情報を公に開示することは想定されないから、当該要件を満たさないのである。

では営業秘密侵害罪が成立しない場合であっても、他の刑事犯の類型には該当しないであろうか。タイの刑法が定める秘密に対する罪としては、信書開封罪（刑法 322 条）、職業上の秘密保持義務を負うものによる秘密漏えい罪（刑法 323 条）、事業上の秘密保

³ CIPITC No. 5216/2552 (2008 年 10 月 1 日)

持義務を負うものによる秘密漏えい罪（刑法 324 条）が規定されている。信書開封罪は対象となる情報の類型が、封をしてある他人宛ての手紙等に限定されているから、適用の場面は少ないと思われる。また、職業上の秘密義務を負うものによる秘密漏えい罪は、情報漏えいの主体が医師、薬剤師、弁護士、会計士等に限定されており、一般的な営業秘密侵害の場面では利用できない。他方、事業上の義務を負うものによる秘密漏えい罪については、その対象が「産業、発明、または科学的発見に関する秘密について義務を負い、信任を受け、または知得した者が、自らまたは第三者のために当該情報を開示または利用した場合」に適用があり、比較的広い範囲で適用がありうる。公の開示が要件となっていないことから、営業秘密侵害罪でなく、本罪に基づく起訴が可能な場合もあると思われる。

なお、情報に対する窃盗罪は（刑法 334 条）原則として成立しない（最高裁裁判所, No. 5161/2547）。窃盗罪に該当するためには、当該情報が保存された有体物（紙、USB メモリ、携帯電話端末等）の窃盗として構成しなければならない。

また、刑法以外にもコンピュータ関連犯罪法（Computer-related Crime Act B.E.2550、以下「コンピュータ犯罪法という」）は、コンピュータに対する不正アクセスの罪（コンピュータ犯罪法 5 条）、コンピュータアクセスへの防御措置を不正に開示する罪（コンピュータ犯罪法 6 条）、コンピュータデータに対する不正アクセスの罪（コンピュータ犯罪法 7 条）を規定しており、一点の侵害類型においてはこれらの類型の刑事犯に基づく起訴も検討される。

タイにおいては、刑事手続きを利用して相手方にプレッシャーをかけることが、和解交渉を有利に進め、損害賠償金を回収するうえで非常に重要である。また、侵害者が在職中の従業員である場合には、当該従業員の解雇の可否を検討するにあたって、刑事犯に該当する行為を行ったか否かが一つの大きな分かれ目となる。それらのような場合においては、「公の開示」要件を満たさずに営業秘密侵害罪にあたらない場合であっても、ここに挙げたような各種の刑事犯の類型に該当するか否かを検討することが有益である。

(4) 民事的措置及び刑事的措置のまとめ

以上に述べた民事的措置及び刑事的措置について、日本法と比較して一覧すると以下の表ようになる。

国	民事的措置	刑事的措置
タイ	・当事者間（被害者・加害者）の民事訴訟 ・侵害行為の差止、侵害行為組成物（営業秘密を侵害する材料、装置、道具、またはその他の設備）	・起訴されれば刑事訴訟に移行 ・私人自身による訴追が認められているほか、検察官が起訴した事件の共同訴追者となることも可能

	の廃棄及び損害賠償請求が可能	・1年以下の禁錮刑もしくは20万 バーツ(約70万円)以下の罰金、 またはその両方。
日本	・当事者間(被害者・加害者)の 民事訴訟 ・侵害行為の差止、侵害行為組成物 (営業秘密記録媒体等)の廃棄 及び損害賠償請求が可能	・捜査後、起訴されれば刑事訴訟・ 刑事罰の内容は、個人について は、10年以下の懲役、2000万 円以下の罰金またはこれらの 併科。法人については、10億円 以下の罰金。

(5) 裁判外の救済手続き

ア 調停

営業秘密に関する紛争については、営業秘密委員会への調停申立てが可能である。調停が成立しなかった場合は、訴訟または仲裁に紛争を委ねることができる(法9条)。後記5(3)のとおり、1997年1月から2020年9月までの間に開始した調停の件数は、民事事件16件及び刑事事件6件である。そのうち調整成立に至った事件は民事事件5件及び刑事事件2件にとどまっている。

イ 仲裁

両当事者による合意がある場合には、仲裁を利用することも可能である。

(コラム) 秘密保持義務違反と営業秘密侵害との違い

会社が秘密を保護する方法として代表的なものは、相手方に守秘義務を課すことであろう。従業員との間であれば就業規則、雇用契約、秘密保持誓約書により、取引先との間であれば秘密保持契約により、守秘義務を課することが多い。相手方が守秘義務に違反した場合には、本マニュアルにおいて述べるような営業秘密侵害として権利救済を受ける方法だけでなく、契約上の義務に基づく責任追及を行うことも可能であるが、両者の間では何が異なるのか。契約であれば、本法における営業秘密に該当しない情報についても、当事者間の合意によって自由に守秘義務の対象を定めることができるという点でメリットがある。営業秘密の厳格な要件を満たさずともよいのであるが、それでもなお営業秘密法における保護を受けることにはどのような利点があるのだろうか。

第一に、会社が請求できる対象が異なる。守秘義務違反に基づく請求は、当然ながら契約当事者に対してしか行うことができない。企業秘密の漏えいにおける典型的なパターンは、会社従業員が社内の秘密情報を持出し、競合他社に漏えいする場合や、自ら当該秘密情報を利用して事業経営を行う場合である。このような場合に、雇用契約や守秘義務契約を交わした従業員に対しては契約上の義務違反を問うことができるが、競合他社や当該従業員が自ら事業を行う会社との間では契約関係がないため、守秘義務違反を

問うことができないのである。また、従業員個人には資力がない場合や、情報の破棄を命じたい相手が漏えい先の第三者であるような場合には、契約上の保護だけでは足りないのである。

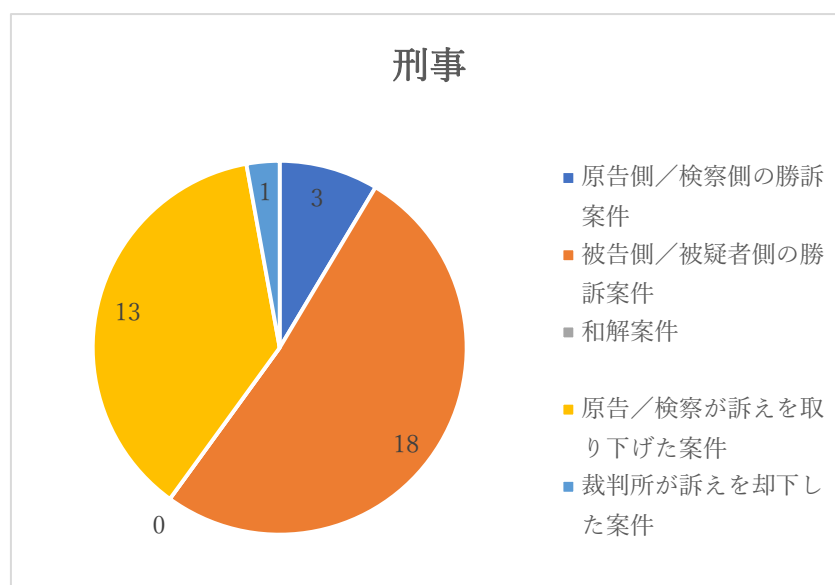
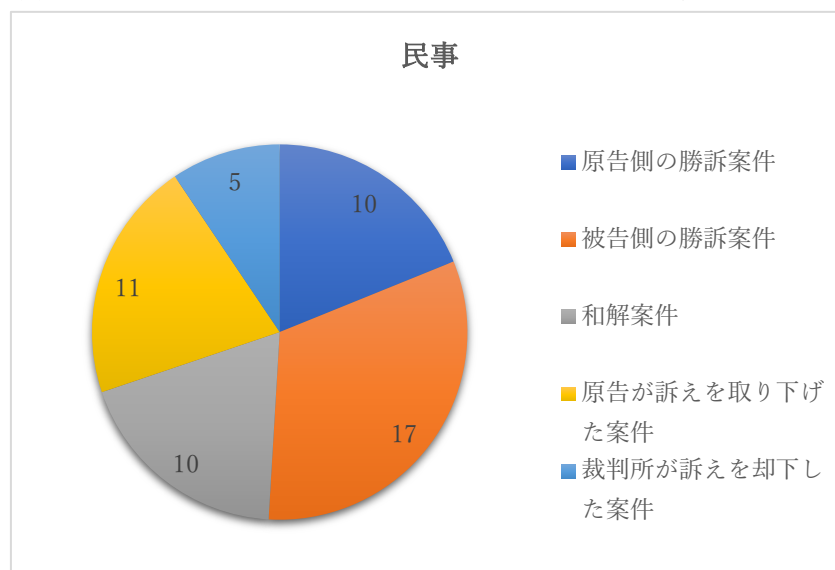
次に、営業秘密侵害の場合には、証拠収集の方法としてインカメラ手続きが利用可能であるメリットも大きい。営業秘密は、秘密であることによって価値を生じる情報なのであるから、裁判によってその内容が公開されてしまつては本末転倒になってしまう場合がありうる。また、情報漏えいの案件においては、情報が漏えいしたことによる損害額を立証することは非常に困難であるが、本法の適用を受けることで、損害賠償額を裁判所が適切と考える金額で認定してしまうことによる立証負担の軽減や、場合によっては（日本とは異なり）懲罰的損害賠償が認められることによる利益も大きい。

最後に、営業秘密の公表に対しては刑事罰が科されているから、刑事事件として警察の助力を得て権利行使が可能であることが挙げられる。民事裁判のみでは、証拠収集を自らの手で行わなければならない、営業秘密侵害を立証するための十分な資料を得ることができないことや、たとえ勝訴判決を得ても相手方が支払いに応じなければ、強制執行まで実行することは原告の大きな負担になること（強制執行の手続きそれ自体に費用と手間がかかるうえに、相手方の財産を特定することができなければ強制執行が空振りに終わってしまう可能性がある。）から、必ずしも実効的な救済を得ることはできない。このため、刑事事件として相手方に警察の捜査が行われれば、証拠資料の収集が容易になるのみでなく、相手方に対して多大なプレッシャーをかけることができ、十分な資力のない相手であっても、親族や金融機関からお金を借りてでも和解による解決を図ろうという動機を与えることができるのである。

5 営業秘密に関する紛争事件の統計情報

CIPITC の協力を得て受領した情報（2020 年 9 月 30 日時点）によれば、1997 年から現在までに至る営業秘密に関する案件総数は以下のとおりである。

(1) 1997 年 1 月から 2020 年 9 月までににおける営業秘密関連紛争



事案の類型	民事	刑事
原告側／検察側の勝訴案件	10	3
被告側／被疑者側の勝訴案件	17	18
和解案件	10	-
原告／検察が訴えを取り下げた案件	11	13
裁判所が訴えを却下した案件	5	1
総計	53	35

(2) 係属中の案件及び控訴中の案件

ア 係属中の案件

民事事件: 7 件

刑事事件: 1 件

イ 控訴中の案件

民事事件: 10 件

刑事事件: 15 件

(3) 調停の案件数

法 9 条に基づく調停が行われた事案の類型と案件数は以下のとおりである。

類型	民事	刑事
調停の開始した案件	16	6
調停が成立した案件	5	2

6 最近の裁判例動向

CIPITC の協力を得て受領した資料 (2020 年 9 月 30 日時点) のうち、有益と思われる裁判例を紹介する。

(1) 民事：営業秘密性が認められたもの

裁判例 No.1-1 (CIPITC, TorPor. 104/2563)

裁判例	CIPITC, TorPor. 104/2563, 2020 年 9 月 8 日
営業秘密の認定	営業秘密に該当する
損害賠償額	10,000,000 バーツ (約 3500 万円)
前提事実	原告らは、タイと日本において太陽光発電所の運営事業を行う事業者らである。原告らは、太陽光発電所の候補地の検討を行うためにデューデリジェンスを実施していた。 被告は、原告らの旧株主かつ取締役 (原告のうち一社と秘密保持契約を締結し、競業避止義務を負っていた) であるが、原告らの競合他社に対し、20 ヶ月以上にわたり、電子メールのやり取り (26 通) を通じて、デューデリジェンス報告書の情報を開示していた。
判決の要旨	裁判所は、以下の理由から、デューデリジェンス報告書が営業秘密にあたると判断した。 (1) 秘匿性

	デューデリジェンス報告書は、公開情報ではなく、一般に知られていない情報が含まれており、一般の人が通常アクセスすることができない情報が含まれている。 (2) 有用性 当該情報は、各分野の専門家の調査・研究・推計・分析から得られる情報であるから、営業情報に該当し、かつ商業的価値を有している。 (3) 秘密管理性 裁判所は、秘密管理性が認められるための「適切な措置」について、原告と同じ立場、状況にある合理的な者の基準に照らして適切であることを指すと判示している。そのうえで、太陽光発電所の用地にかかるデューデリジェンスの結果に関する情報は、投資家に対して開示する必要があることに照らして、たとえば開発中の新薬や化合物の情報等に比すれば、厳格な秘密管理措置までは求められないとしている。本件においては、以下の秘密保持措置がとられていることを事実認定したうえで、デューデリジェンス報告書が秘密情報であることを認めた。 ア 情報にアクセスできる者の制限 イ 情報へのアクセスのためのパスワード設定 ウ 秘密保持契約及び競業避止義務契約の締結 エ 原告の取締役である被告との間には、信頼関係と忠実義務があること
コメント	秘密管理性が認められるための「適切な措置」について、原告と同じ立場、状況にある合理的な者の基準に照らして判断する旨が示されている。 タイにおける営業秘密侵害事案における損害賠償として認定された最高額である。

裁判例 No.1-2 (最高裁判所, No. 7769/2557/ CIPITC, TorPor. 98/2551)

裁判例	最高裁判所, No. 7769/2557, 2014 年 6 月 17 日 CIPITC, TorPor. 98/2551, 2008 年 7 月 21 日
営業秘密の認定	営業秘密に該当する
損害賠償額	1,000,000 バーツ (約 350 万円) 及び年率 7.5%の遅延損害金
前提事実	原告は製造業を営む法人である。

	被告ら数名は、原告との雇用関係のある従業員である期間に、原告が製造するものと類似の液体ボトル製造機械の製造及び販売を営む株式会社を共同で設立した（同株式会社も本事案の共同被告とされている）。被告は、原告の機械部品の生産計画や営業情報を持出して業務に使用しており、警察の捜査も受けていたが、原告と同じ請負業者に委託を行い、原告の機械部品の生産計画を使用したうえで、原告と同種の機械部品を製造していた。
判決の要旨	(1) 営業秘密に該当する情報 (1-1) 機械部品の製造計画 機械部品の製造計画は、一般に広く知られておらず、かつ当該情報に関係する者の間でも一般にアクセス可能でないとして営業秘密と認められた。また、当該製造計画を秘密として維持するための適切な措置として以下のような事実が認定されている。 ①製造計画書はコンピュータ上に保存されており、プリントアウトされた書面（1-2 部）は鍵のかかった部屋（1-2 室）に保管されていること、 ②当該情報に関連する業務を担う従業員のみが当該ファイルにアクセスすることができるが、閲覧のためには、利用申請書を提出しなければならない、当該ファイルは必ず当日中に返却しなければならないこと。 なお、機械のうち 20%に相当する部品を第三者である請負業者が製造しており、当該業者が、部品の修理・交換の際に参照するためコピーをとっていることも前提となる事実として認められている。この点について裁判所は、当該請負業者において製造されているのは最終製品の 20%に留まることから、当該部分のコピーのみによっては実際に機械を作ることはできず、秘匿性は失われていないと認定している。 また、被告が当該情報を持ち出すことができたのは、被告が原告の工場長であって機械の全部品の情報を把握しており、退社時に受けることとされている検査の義務を免除されていたからである。 裁判所は、原告がファイルへのアクセスを制限したり、ファイルの保管を制限する措置をとったりしても、被告を情

	報から遮断することはできなかったのであるから、原告が情報を秘密にするためにとった措置は十分であったと認定している。 (1-2) 顧客(機械購入者)に関する情報 顧客の氏名、購入した機械の種類、納入日等を含む営業情報は、一般的に関係する者の間では広く知られておらず、またはアクセスすることができない情報であり、秘密が保たれることによって商業的に有益であって、かつその秘密を保持するための適切な措置が講じられていると解されるとして、営業秘密に該当すると認定された。 ここにいう適切な措置とは、①当該情報がコンピュータに保存されたうえでパスワードが付され、②セールスアシスタントマネージャーと取締役のみがファイルにアクセスすることができたことを指している。また、③ハードコピーのファイルは、セールスアシスタントマネージャーの施錠されたキャビネットに格納されており、他の従業員は当該ファイルや情報にアクセスすることができなかった。そして、④その他の従業員が保証期間に関する情報等を知るためには、当該セールスアシスタントマネージャーに電話で確認しなければならなかった。 (2) 営業秘密に該当しない情報 (2-1) 見積書記載の情報 見積書に記載されている情報について、秘密として保持するための適切な措置があることが立証できていないとして、秘密管理性の要件を欠くために営業秘密として認められなかった。 (2-2) 顧客(医薬品メーカー)の氏名、連絡先を含む情報 医薬品メーカーの顧客連絡先情報は、当該情報に関係する者が一般的に入手することができるものであることから、秘匿性の要件を欠くとして営業秘密性が否定された。 (2-3) 付属部品の製造業者の情報 広告等で入手可能な情報であって、当該情報に関係する者が一般的に入手可能であるため、秘匿性の要件を欠くとして営業秘密性が否定された。
コメント	被告の主張の中で興味深いものとして、原告が従業員に対して用紙の再利用を奨励しており、再利用に供された紙の

	中には、製品の製造計画に関する書面も含まれていたとの主張がある。最終的に被告はこの事実を立証できなかったため、判決の基礎となる事実には含まれていないものの、実際に営業秘密に該当する情報が記載された書面を再利用していた場合には、秘匿性や秘密管理性が否定されていた可能性がある。会社が、いわゆるセーブ・アース・ポリシー（save earth policy）を実施する場合には、再利用する用紙について留意が必要である。 また、判決の要旨 1-1 に記載のとおり、外部委託業者の情報利用についても注意が必要である（本事案では外部委託業者へ開示する情報が限定的であったために秘匿性の要件は失われなかった）。具体的には、当該外部委託業者との間で秘密保持契約を締結するほか、文書の使用についてコピー制限をかけたり、使用後の返却・破棄義務を課したりすることが必要である。
--	---

裁判例 No.1-3 (特別専門事件控訴裁判所, No. 732/2560/ CIPITC, TorPor. 8/2560)

裁判例	特別専門事件控訴裁判所, No. 732/2560, 2017 年 7 月 18 日 CIPITC, TorPor. 8/2560, 2017 年 1 月 31 日
営業秘密の認定	営業秘密に該当する（争いなし）
損害賠償額	150,000 バーツ（約 52.5 万円）及び年率 7.5%の遅延損害金
前提事実	原告は不動産開発業者であり、顧客の氏名、住所、連絡先、行動、態度、嗜好(スタイル)といった顧客情報を所有している。 被告 1 は、原告の IT 部門に勤務するシステムアナリストであって、システムやデータの管理、顧客情報を含むシステム内の情報へのアクセス管理権限者であり、原告からの指揮のもとで、許可された範囲内において営業秘密の管理、不正アクセスに対するセキュリティ、従業員による当該情報への不正アクセス禁止等の業務を行っていた。被告 1 は、原告のシステムに不正にアクセスし、顧客情報を電子メールにより外部の第三者である被告 2 に送信した。被告 2 はさらに当該情報を第三者に対して 6 回にわたり販売した。
判決の要旨	本件においては、売買された顧客情報が営業秘密に該当することそれ自体は争点とならず、損害額の算定が争点とな

	った。それぞれの費目に対する第一審裁判所の判断は以下のとおりである。なお、原告は被告 1 に対する訴えを取り下げたため、被告 2 に対する損害賠償額についてのみ判断している。 (1) 顧客基盤を築くための広報活動に対する損害：15 万パーツ。本事案では当該費目のみが損害として認められた。 (2) 顧客情報の価値喪失：認められない。裁判所は、購入者が顧客情報から価値を得たことが、顧客情報の価値を毀損したこととの関連性を立証できていないとした。 (3) 調査のための費用：認められない。裁判所は、被告 2 が原告に対して証拠を開示したと認定している。 (4) 懲罰的賠償：認められない。法 13 条 3 項に基づく懲罰的賠償が認められるためには、営業秘密が当該行為によって営業秘密としての性質が失われていなければならない。本件においては、営業秘密は一般に開示されておらず、自己の目的のために使用する者らに販売され、原告のデータベースから営業秘密が消失したのでもないから、当該情報は依然として営業秘密であると認定された。 (5) 被告 2 が営業秘密の使用をやめるまで月額 50 万パーツの損害賠償：認められない。裁判所は、被告 2 がもはや原告の営業秘密を使用していないと認定した。
コメント	懲罰的損害賠償請求の可否が争点となった事案であるが、要件の一つである当該行為によって営業秘密性が失われたことを満たさないと判断された。

裁判例 No.1-4 (CIPITC, TorPor. 18/2563)

裁判例	TorPor. 18/2563, 2020 年 2 月 13 日
営業秘密の認定	営業秘密に該当しうる（最終的に判断せず）
損害賠償額	なし
前提事実	原告は、不動産仲介業を営む法人である。原告は、顧客一般に提供する不動産案件情報を「リスティング・オンライン」と呼ばれるシステム上で収集している。「リスティング・オンライン」においては、アパート、住宅、宅地、土地、マンション等の不動産に関する情報が掲載されており、物件の所在地、価格、募集価格等の詳細や情報が掲載されて

	いた。原告は、当該情報にアクセスできる権限を有する者を限定し、当該情報にパスワードを付していた。 被告は、原告において約 18 年間勤務した住宅アドバイザーであった。被告は、原告と同種事業を営む会社に勤務することを企図して、原告を退職する前に「リスティング・オンライン」の情報をコピーしたうえで、会社のメールアドレスから、自己のメールアドレスに当該情報を送信していた。
判決の要旨	(1) 営業秘密性に関する判断 裁判所は、「リスティング・オンライン」に掲載されている情報は、原告が不動産の売却を希望する顧客を通じて、原告が収集したものであるから、不動産の種類と金額に関する情報は公開情報ではないこと（秘匿性）、不動産市場における商業的価値を有するものであること（有用性）を認めている。さらに、原告は、(ア)当該情報へのアクセスについて本人認証が行われていること、(イ)更新の必要があるパスワードが設定されていること、(ウ)データベースへのアクセスのためには、システムの管理者を経由してパスワードを設定しなければならないこと等を指摘して、営業秘密を不正アクセスから保護するための適切な措置を講じていると評価している（秘密管理性）。したがって、当該情報は営業秘密に該当しうると考えられる。 ※もともと、後記のとおり営業秘密への侵害行為が存在していないことから、営業秘密性について確定的な判断を示していない。 (2) 侵害行為の認定 裁判所は、以下の事情を考慮して、被告が原告の営業秘密に対する侵害行為を行っていないと判断した。 ア 被告は、原告における住宅アドバイザーとして情報にアクセスし、所持する権限を有していた。したがって、当該情報を不法に配布したり、使用したりしたものではないこと。 イ 当該情報は、被告が営業担当者として保持してはいけないような機密情報ではないこと。
コメント	判決のうち「(2) 侵害行為の認定について」は、裁判所がいずれの要件に照らして営業秘密侵害性を否定したのか、判

	決文のみからは明らかでない。おそらくは法 6 条における「正当な商業手法に違反する行為であること」の要件を充足しないと判断したものと考えられる。そうであるとすれば、業務上取扱っている営業秘密を、自己のメールアドレスに送信する行為が、正当な商業手法に違反するとまではいえないと判断したことになる。 企業側の防衛策としては、会社の情報を個人のメールアドレスに送信することが、「正当な商業手法」に違反する行為にあたるよう、雇用契約または就業規則において、会社の営業秘密を社外の私用アカウントや SNS を通じて送信しないよう義務付けておく必要がある。
--	--

(2) 民事：営業秘密性が否定されたもの

裁判例 No. 1-5 (CIPITC, TorPor. 91/2563)

裁判例	CIPITC, TorPor. 91/2563, 2020 年 8 月 10 日
営業秘密の認定	営業秘密に該当しない
損害賠償額	なし
前提事実	原告は、遠隔防犯カメラ設備の販売、設置、及びメンテナンスを行う事業者である。 被告は、原告の支店における支店長であったが、退職後に原告と同様の事業を開始し、Google 社が提供する「Google マイビジネス」に掲載されている原告の商品及びサービスに関する広告情報を自らのものとして持出し、原告の許諾を得ることなく、自らの事業に利用していた。 ※「Google マイビジネス」とは、事業者が商品やサービスを宣伝するための画像や文章をアップロードし、Google 検索や Google マップを利用する顧客が、店舗の所在地や種類を検索できるようにするためのプラットフォームである。 本件において被告は、当該「Google マイビジネス」の情報は自らのアカウントにおいて登録されているのであって、当該情報はむしろ自己の保有する営業秘密であると主張して、原告に対して当該情報の利用を停止するよう反訴を提起した。

	なお、被告の雇用契約書においては、雇用中に行われた著作物の所有権に関する規定はあったものの、競業避止義務は定められていなかった。
判決の要旨	裁判所は、以下の理由から「Google マイビジネス」に掲載されている情報が、営業秘密に該当しないと判断した。 (1) 秘匿性: 原告は、消費者及び顧客が Google 検索や Google マップを利用する際に、店舗情報に容易にアクセスできるよう、オンラインプラットフォーム上で当該情報を宣伝しているものである。したがって、原告には、当該情報を秘密に保つ意図はなく、むしろ公表したいと考える性質の情報といえる。 (2) 有用性: 当該情報は、公開されることに商業的価値があるのであって、秘密にすることによって商業的価値が生じるものでない。 (3) 秘密管理性: 当該情報の秘密を保持するための措置が講じられていない。
コメント	本判決の結論自体は、検索エンジンにおいて公開される情報が営業秘密に該当しないとするものであって、当然のものともいえる。 なお、営業秘密とは直接関連しないものの、本判決では職務著作の権利帰属について若干の言及があるから紹介する。タイの著作権法 9 条は、「雇用の過程において、従業員である著作者が作成した著作物については、これに反する書面による合意がないかぎり、雇用主が雇用の目的において当該著作物を公衆に伝達する権利を有することを条件として、<u>著作権は著作者に帰属する</u>」と規定している。日本の著作権法では、「従業員が会社の指示にもとづき職務中に創作した著作物は<u>原則として会社に帰属する</u>」ところ（日本の著作権法 15 条 1 項）、取扱いが真逆になるから注意する必要がある。従業員による著作物の創作が想定される業務に関しては、就業規則や雇用契約において著作権の帰属について明確に規定しておくべきである。

裁判例 No.1-6 (最高裁判所, No. 1323/2560/ CIPITC, TorPor. 102/2557)

裁判例	最高裁判所, No. 1323/2560, 2017 年 3 月 6 日

	CIPITC, TorPor. 102/2557, 2014 年 10 月 10 日
営業秘密の認定	営業秘密に該当しない
損害賠償額	なし
前提事実	原告は通関業務を行う物流会社である。 被告 1 は原告の元取締役である。本件は、被告 1 が、競業他社である被告 2 に対して、原告の顧客及びサプライヤー情報（名称、住所、合意価格）を開示したとして、損害賠償請求を求めたものである。
判決の要旨	最高裁判所は、以下の理由から被告 1 が被告 2 に開示した情報が、営業秘密に該当しないと判示した（第一審の事実認定もおおむね同様である）。 (1) 原告は、当該情報をコンピュータ上に保存しているが、見積書についてはそのコピーをプリントアウトしている。プリントアウトされた資料はキャビネット内のファイルに保管されており、すべての従業員がアクセスできるようになっていた。また、コンピュータ上に保管されていた情報にはパスワードが付されていたが、パスワードは当該コンピュータのモニターに貼付けて公開されていたため、実際にはどの従業員も情報にアクセスできるようになっていた。 (2) 文書の形態であれ、コンピュータに保存された電子媒体の形態であれ、情報を管理している担当者以外の従業員が情報にアクセスできることは、原告が当該情報を秘密として保持するための適切な措置を講じていなかったことを示すものであって、営業秘密とは認められない。 また、裁判所は、秘密を管理するための適切な方法として以下の例を挙げている。 (1) 営業秘密となる情報を特定し、維持するための内部規則を制定し、実施すること (2) 文書を機密情報としてマークすること (3) 従業員が会社の秘密を漏らさない雇用契約を締結すること
コメント	会社が秘密にしたい情報に対して、実効的な秘密管理措置（アクセス制限）が行われなければ、営業秘密として認められないことを示す事案である。

(3) 刑事：営業秘密性が認められたもの

裁判例 No.2-1 (CIPITC, No. 5275/2549)

裁判例	CIPITC, No. 5275/2549, 2005 年 3 月 18 日
営業秘密の認定	営業秘密に該当する
禁錮及び罰金	なし（無罪）
前提事実	被害企業は、自動包装機の製造事業を主たる事業とする株式会社である。被疑者 1 乃至 5 は、かつて被害企業の工場に勤務し、自動包装機にかかる業務を担当していた者である。被疑者らは、被害企業での雇用期間終了後、被害企業と同種の業務を行う株式会社（被疑者 6）を設立し、被害企業と同様の業務を行った。また、被疑者らは、被害企業の機械の製造工程や顧客リスト等、被害企業の営業情報を持出したうえで、新会社における自らの業務に利用していた。
判決の要旨	裁判所は、被害企業の機械製造工程及び顧客リストは、それが一般に広く知られておらず、一般的に係る者の間ではアクセスできないこと、またその計画を秘密として維持するための適切な措置が講じられていること等の理由から、被害企業の営業秘密に該当することを認定した。 しかしながら、被疑者らの行為は、被疑者ら 6 名の間で開示されたのみであって、法 33 条が規定する侵害行為の要件である「営業秘密を公に開示したこと」にあたらないと判断した。
コメント	営業秘密を公に開示したことの要件について具体的な判断を示した事案である。具体的な判断基準は示されていないものの、 <u>開示先が特定少数にとどまる限りにおいては、本罪の構成要件を構成しないものと考えられる。</u>

(4) 営業秘密性が否定されたもの

裁判例 No.2-2 (最高裁判所, No. 19015/2555/ CITIPC, Or. 5035/2553)

裁判例	最高裁判所, No. 19015/2555, 2012 年 12 月 17 日 CITIPC, Or. 5035/2553, 2010 年 12 月 14 日
営業秘密の認定	営業秘密侵害に該当しない
禁錮及び罰金	なし（無罪）
前提事実	被害企業は、セラミックタイル及びモザイクタイルの製造

	事業を営む株式会社である。被疑者は、被害企業の工場長として勤務していた者であるが、被害企業における雇用期間終了後、被害企業と同様の事業を営む新会社を設立し、被害企業と同様の事業を行っていた。その際、被害企業の商業情報を持出して新会社の事業に利用した。
判決の要旨	(1) 金型 (1-1) 金型模型：被害企業は、金型模型に関する営業情報を金型製造会社の開示しており、当該金型製造会社との間で機密情報を保持することについて何ら合意することなく、互いの信頼関係のみに依拠して情報を開示していることから、秘密管理性の要件を満たさず営業秘密に該当しない。 (1-2) セラミックタイルの型紙及び模様：被害企業のセラミックタイルの製造は、ヨーロッパの様々な広場の街路にある床タイルをヒントにしたものにすぎず、セラミックタイルの型紙及び模様は営業秘密とはいえない。また、当該セラミックタイルを製造して流通させた場合には、当該セラミックタイルの模型及び模様は、その性質上公知のものとなるのであって、セラミックタイルの模様は、広く一般に知られており、これらの情報に係る者の間で入手することが可能である。 (2) 生産方式 被害企業は、当該情報を秘密として保持するための適切な措置を立証していないため、生産方式は営業秘密に該当しない。被害企業における秘密管理の方法は以下のようなものであった。 (2-1) 製造担当の従業員だけでなく、工場内の一般従業員も製造にどのような成分を使用するのか知っていた。 (2-2) 生産ラインは屋外にあって、工場に勤務するすべての従業員が生産ラインにアクセス可能であった。また、工場内には、どの領域が機密情報で、どの領域がそうでないかを示す標識等は存在しなかった。 また、上記第一審の事実認定に加えて、最高裁においては、被害企業が、秘密情報を保持するための措置として、従業員が秘密情報を開示することを禁止する就業規則を作成していることを認めつつも、就業規則上の規程があることの

	みをもって、秘密保持のための適切な措置があるとみなすには不十分であることを判示している。
コメント	従業員が機密情報を開示することを禁止した就業規則を制定するのみでは、秘密管理性を認める十分な要素となりえない。すなわち、いわゆる組織的安全管理措置を施すのみでは足りず、その他に技術的安全管理措置（アクセス権の設定、パスワードの付与）、物理的安全管理措置（施錠された部屋やキャビネットにおける情報保管、入退室管理、持ち物検査）、人的安全管理措置（従業員教育）が必要であるということがいえる。 なお、セラミックタイルの型紙や模様については、営業秘密に該当しないとしても、別途著作権法により保護されないかを検討する必要もあるだろう。

(5) 裁判例 No.2-3 (最高裁, No. 10217/2553/ CIPITC, No. 3662/2548)

裁判例	最高裁, No. 10217/2553, 2010 年 11 月 9 日 CIPITC, No. 3662/2548, 2005 年 9 月 1 日
営業秘密の認定	営業秘密に該当しない
禁錮及び罰金	なし（無罪）
前提事実	被害企業は、溶鉱炉業界におけるバーナー機器及び燃料制御システムの製造及び販売を主たる業務とする法人である。被疑者らは、被害企業の営業部門の営業員として勤務していた（被疑者 1 及び被疑者 2）。被疑者 1 及び被疑者 2 は、被害企業に在職中、被害企業の顧客リストを別の第三者（被疑者 3）に開示し、さらに被疑者 3 が、被害企業の競業相手である会社（被疑者 4）に対して、当該情報を使用させる意図をもって開示した。なお、被害企業が、被疑者 1 及び被疑者 2 との間で締結していた雇用契約書には、雇用人の情報の開示を禁止する旨の規定があった。
判決の要旨	原告の顧客リストは、以下の理由から、営業秘密とは認められない。 (1) 秘匿性：当該顧客リストは、被害企業のウェブサイト上において、一般の人々がアクセスできるようにオンライン上で公開されていた。 (2) 秘密管理性：当該顧客ファイルは、営業部と経理部の両

	部門に保管されており、両部門の担当者は常にこの情報にアクセスできるようになっていた。また、当該文書の所有者及び使用者を特定するために文書を監視・管理する体制も特段とられておらず、コンピュータ上のデータは一切暗号化されていなかった。
コメント	

第2章 漏えい対策実践編

1 タイにおける営業秘密管理の3ステップ

本章では、会社が営業秘密を保護するためにとるべき対応策について論じる。特に、第1章において言及した営業秘密の要件のうち「秘密管理性」について、過去の裁判例において認められた事例、あるいは認められなかった事例を参照しつつ、具体的にどのような対応策が求められるかについて解説している。

なお、営業秘密法上、秘匿性や有用性が認められないために営業秘密には該当しえない情報であっても、会社として外部に知られることを避けたいと考える企業秘密も当然存在するはずである。たとえば会社内のすべての従業員が承知している情報であっても、社外の第三者には知られてはならない情報、社内的にはあえて営業秘密と同列に扱うことで、情報保護・流出対策を図ることも十分合理的な方策であるといえる。

したがって、本章で述べる漏えい対策を実施するうえでは、必ずしも営業秘密の定義と概念にとらわれる必要はなく、「どの情報を秘密に保ちたいか」という実質的な価値判断に基づき、「情報の選別」と「体制の整備」を図るべきである。

そこで、本章では営業秘密管理のための各種対応策を3ステップに分けて詳述する。すなわち、保護すべき情報の選別（ステップ1）、現状の情報保護体制の分析とあるべき保護体制のギャップの認識（ステップ2）、そして当該ギャップを埋めるための体制整備の実施である（ステップ3）。また、これらの一連の取り組みは、普段から、そして、不断に取り組むことも重要である。

(1) ステップ1：保護すべき情報の選定及び重要度の選別

前記裁判例 No.1-6 (最高裁判所, No. 1323/2560/ CIPITC, TorPor. 102/2557)が示す通り、秘密管理体制の構築における主要な対応策は、以下の3点が中心となる。

- (1)営業秘密となる情報を特定し、維持するための内部規則を制定し、実施すること
- (2)文書を機密情報としてマークすること
- (3)従業員が会社の秘密を漏らさない雇用契約を締結すること

また、上記(1)乃至(3)のいずれの対応をとるにしても、そもそもどの情報を営業秘密として取扱うのかが特定されていなければならない。

なお、就業規則や雇用契約において、従業員が業務に際して取扱う情報はすべて秘密として扱うべしとする例も散見されるのであるが、このような規定のみでは従業員が個々の場面においていかなる情報をどのように取扱うべきか判断することができない。したがって、会社として、具体的にどのような情報を営業秘密（あるいは企業秘密）として扱わなければならないかを明示する必要がある。

例えば、製造業であれば「製造工程」や「図面」のような技術情報を保護する必要があるし、医薬品や化学物質を取扱う事業者であれば「化合物の生成や配合にかかる情報」を保護する必要があるだろう。また、業種に関わりなく「顧客リスト」

や「見積り情報」などは、多くの場合、対外的に秘密にしたい情報であろう。漠然と重要な情報というのではなく、これらの情報だと分かるようにリストアップしなければならない。

(2) ステップ2：現状の管理体制の確認

ステップ1において保護すべき情報を定めたら、次のステップとしては、現状の管理体制を精査して、情報管理の観点からどのような点が不十分であるかを見極める必要がある。

現状の管理体制を確認するにあたっては、以下のようなセルフチェックシートの活用が役立つであろう。その際は、各社の事業形態や、秘密としたい情報の類型、情報の保管される方法や使用される方法により、チェックすべき具体的な項目にはある程度の差が生じるが、以下のようなセルフチェックシートを利用することで、典型的な対応項目については漏れなく検討することが可能になる。

セルフチェックシート	
1. 秘密の指定： 会社として、その類型の情報を営業秘密として指定するのかを定め、その情報が含まれている文書やファイルを特定することは、秘密管理体制の構築のために必須である。そのうえで、情報の類型・重要度に応じて当該情報にアクセスできる部署や役職について指定しなければならない。	
1-1	☐ 秘密保持の必要性のある保有情報をリスト化している
1-2	☐ 当該保有情報の区分を行ったうえで、特に秘密保持の必要性の高い情報や営業秘密として管理すべき情報を特定している
1-3	☐ 秘密の重要度に応じたアクセス権者を定めている
2. 管理方針の策定： 上記1で指定した情報類型とアクセス権者について、社内規程等の形態で文書化されていないなければならない。また、定めたルールを実行するための責任者（責任部署）の設置も必要となる。社内規程については、日本の本社で同種の規程を策定している場合には当該規程を参照しつつ、タイ現地事業用にアレンジしていくことも考えられる。	
2-1	☐ 現地の法令に基づいて作成された営業秘密管理規程または管理マニュアルが策定されている
2-2	☐ 各拠点において営業秘密管理責任者を選任している
3. 物理的管理（執務室）： 会社が営業秘密として指定した文書については、ファイル上それとわかるような表記をしたうえで（「秘密」「厳秘」の透かしを付す等）、紙媒体であれば施錠可能なキャビネットに保管するといった対応が必要である。また、原本のみでなくコピーが流通	

してしまうことがないよう、複製制限やトラッキングを可能にしておく措置が望ましい。	
3-1	☐ 秘密情報を含む記録媒体に「controlled copy」等の秘密表示がされている
3-2	☐ プリンターの利用者記録を確認することができる
3-3	☐ 秘密情報を、一般情報と分離して保管し、紙媒体等は施錠可能なキャビネットで保管されている
3-4	☐ 秘密情報の持出しの際の盗難防止策がとられている
3-5	☐ 秘密情報の複製を制限するルールが定められている
4. 物理的管理（生産現場等）： 執務室と異なり、取引先候補、外部業者、見学者といった部外者が立ち入る可能性があるため、特に入退室管理に留意する必要がある。また生産現場において掲示されている印刷物は、工場で勤務する従業員すべての目に触れることとなるから、秘密を保つことは難しくなる。技術情報の表示には注意すべきである。	
4-1	☐ 外部の者が立ち入る際には部外者であると認識できるようバッジ等をつけている
4-2	☐ 工場内の情報が部外者に見えないようゲートや扉で適切に仕切られている
4-3	☐ 工場内では携帯電話を私用できる職員が限られている、または禁止されている
4-4	☐ 重要度の高い秘密情報を扱うエリアは、一部の社員のみに入入りを認めている
4-5	☐ 立ち入り制限エリアを管理している（警備員の配置、入退室記録等）
5. 技術的管理： 電子ファイルについては、ファイル名自体に「厳秘」と付すなど、一見して、秘密情報と分かるようにする工夫が重要である。その上で、秘密情報を含むファイルについては、アクセス制限とパスワードの付与が基本的な対応となる。なお、従業員間でパスワードを共有してしまっている場合には、実質的に秘密管理が行き届かなくなるから、パスワードを他者に教えないよう周知徹底する必要がある。	
5-1	☐ 秘密情報を含むファイルについて、重要度に応じて「秘密」、「厳秘」といった表記をしている。
5-2	☐ 従業員の PC にパスワードを設定している
5-3	☐ チャットアプリの使用を禁止・制限している（とりわけ、秘密情報を含むファイルについて、チャットアプリでのやり取りを制限している）
5-4	☐ 私物の USB メモリ等記録媒体の利用を禁止・制限している

5-5	☐ 秘密の度合いに応じて管理者の特定、アクセス権者の限定をしている
5-6	☐ 複製使用後、情報が読み取れないような廃棄方法が徹底されている
6. 人的管理： 就業規則、雇用契約、秘密保持誓約書により守秘義務を課すことと、秘密保持に関する教育・研修を徹底することが必要である。なお、競業避止義務を課すうえで経済補償金を設定することは必須でないものの、義務の内容や範囲によっては検討を要する。	
6-1	☐ 定期的に研修を行い営業秘密保護の重要性を周知喚起している
6-2	☐ 雇用契約で営業秘密保持を定めている
6-3	☐ 秘密保持誓約書を提出させている（秘密保持範囲と守秘期限を定めている）
6-4	☐ 守秘義務に違反した際の懲罰規定が明記されている
6-5	☐ 退職者に対して競業避止義務を定めている
6-6	☐ 競業避止義務を定めた退職者に対して、経済補償金を設定している
6-7	☐ 退職者による必要資料の返還がなされたかリストをもとに管理している
7. 取引先管理： 営業秘密の提示が想定される取引先との間では、常に秘密保持契約を締結することが必要である。会社としては、秘密保持契約のひな形を作成するべきであり、取引先がドラフトした秘密保持契約を利用する場合には、必ずその内容のレビューを行ったうえで締結するべきである。	
7-1	☐ 秘密保持契約を締結している
7-2	☐ 秘密に該当する情報を明記している
8. 侵害に備えた証拠確保： 営業秘密が漏えいした場合、その漏えい経路が分からなければ情報漏えいを止めることができないし、責任追及すべき相手も分からないこととなる。ただし、プライバシー侵害（職場といえども各従業員には守られるべきプライバシーが存在する）となりうることに注意して、業務上必要な範囲でモニタリングを行う必要がある。	
8-1	☐ 秘密度の高いエリアには監視カメラを設置している
8-2	☐ メール送信記録、ウェブサイトの閲覧記録が確認できる

(3) ステップ3：対象別の体制整備

ステップ1（保護すべき情報の特定・選別）、ステップ2（現状の管理体制の確認・点検）を行ったら、最後のステップとして、保護対象とすべき情報に応じた、体制の整備を図る必要がある。この際には、営業秘密として法的保護を確保する必要がある情報や、個人情報、安全保障関連技術情報など「厳格な管理」が求められるも

の、これら以外の企業として秘密にしておきたい情報のような「相応の管理」でも足りるかもしれないものなど、情報の内容・特質と秘密確保に対する企業としての意向などを踏まえつつ、情報の保護と活用、管理コストなどのバランスも勘案し、適切な体制を整備・構築することが肝要となる。

ア 情報管理体制の専門部署/担当者の設置

会社の営業秘密保護体制を整備するうえで、営業秘密の取扱いについて実務上の判断を行い、秘密管理に関するルール策定、管理運営、監査教育を行うための人的体制を整える必要があるから、情報管理を担当する部署や担当者を選任すべきである。また、会社全体としての営業秘密に対するポリシーや運用を明確にするため、秘密情報管理規程を策定することが望ましい。

イ 人事労務体制の整備、従業員の管理

(ア) 従業員の守秘義務を課するための契約締結

従業員に対しては情報管理のための守秘義務を課さなければならない。具体的には、①就業規則、②雇用契約、③個別の秘密保持誓約書の三段階で秘密保持義務を課することが望ましい。特に、①就業規則においては、秘密保持義務を課すのみにとどまらず、違反した場合の懲戒規定がなければ実効性に欠くこととなるから、懲罰についても規定する。また、②雇用契約においては就業規則と異なり、個々の従業員ごとに異なる契約内容を設定することができるから、特にマネジメントクラスの従業員に対しては他の従業員よりも期間の長い秘密保持や競業避止義務を課することが可能である。なお、①及び②に共通して重要なことは、退職後の守秘義務についても明示的に規定することである。実際に営業秘密の漏えいが問題となるのは、会社の退職後であることが多い（前記裁判例 No.1-4 (CIPITC, TorPor. 18/2563)のように競業他社に転職するケースや、裁判例 No.1-2 (最高裁判所, No. 7769/2557/ CIPITC, TorPor. 98/2551)のように自ら同種の事業を営む会社を立ち上げるケース等）。雇用期間中の守秘義務のみでは足りず、退職後においても、具体的にどの程度の期間にわたって、会社の情報に対する秘密保持義務を負うのか、明記しておく必要がある。③個別の秘密保持誓約書については、従業員の退職時に提出させることや、従業員が重大な営業秘密に触れる役職に就いたり、そのようなプロジェクトメンバーとなったりするときに提出させることが想定される。具体的な場面に即して作成する誓約書であるから、秘密とすべき情報の対象が明確であることのほか、従業員本人に対して秘密保持義務を強く意識づけるという事実上の効果においても重要である。

(イ) 従業員に対する教育・研修

従業員に対しては守秘義務を課すのみでなく、その守秘義務を守らせるための教育と研修を徹底することも必要である。これは一度説明すれば十分というものではなく、入社時教育、管理職への昇進時研修、定期的な社内研修（社外の専門家に委託する方法でもよい）など複数の機会を通じて、当該従業員の職務や職位が変わるごとに、繰り返し意識づけることが重要である。

（コラム）SNS 利用の制限について

多くの日系タイ企業に共通する情報管理上の悩みとして、タイのローカル従業員が、業務の一環として SNS (Social Networking Service) を利用していることが挙げられる。タイにおいては、Line を始めとするコミュニケーションアプリの利用率が高く、家族や友人とのプライベートのやりとりのみならず、同僚同士の業務連絡や、外部事業者であるサプライヤー担当者とのやりとりにおいても、コミュニケーションアプリを通じて行っている場合がある。

業務において SNS を利用することの問題点として、当該 SNS が、会社の管理する端末ではなく、従業員個人の保有する携帯電話端末にインストールされたアプリや、当該従業員が個人で作成したオンラインアカウントに紐づいてしまっていることがある。すなわち、(i)従業員個人が保有する端末は、会社が支給する業務用端末と比較してセキュリティが不十分になってしまう可能性があり、またセキュリティ水準を管理・統一することが困難であることから、サイバー攻撃を受けるリスクがあること、(ii)情報漏えい等が生じた場合における情報のトラッキング・モニタリングが困難となること、(iii)私用端末の紛失・盗難リスクがあること、(iv)退職時における企業情報の破棄・返還が難しく、退職後にも情報を保有し続けてしまうリスクがあることが挙げられる。

もっとも、業務上の SNS 利用が一般化しつつあるタイにおいては、SNS 利用を一律に禁止するような施策は、現場の業務運用上もはや現実的ではない場合もある。すると、現地の実務慣行に適合しないルールを制定したところで、かえってルールは形骸化してしまい、会社の規律や管理が及ばないという事態を招く可能性がある。したがって、タイで事業を行う日系企業としては、むしろ SNS がビジネスにおいて大きな役割を果たしていることを認め、情報管理上のリスクがあることも踏まえて、SNS を用いてよい場面とそうでない場面との区分けを行い、従業員に対しても周知徹底することが重要である。たとえば見積書や契約等のファイルには重要な情報が含まれることが典型的に多いため、SNS でファイル送信を行うことを禁止して、SNS は打ち合わせのスケジュール調整や単純な連絡事項の伝達にのみ使うといった方策が考えられる。ただし、秘密情報の管理を特に厳格に行わなければならない場合（研究施設に勤務する従業員等）においては、携帯電話の持込みを禁止する等、通常よりも一層厳格な処置をとることが望ましい。

会社の秘密情報を SNS で公開してしまわないようにする注意喚起も必要である。日

系企業からの相談例としては、タイのローカル従業員が海外出張や地方出張の様子を SNS に投稿してしまい、会社の事業戦略や協業パートナーに関する方針が推測できる状況になってしまった、あるいは事業所の写真を SNS に投稿して重要な秘密情報が映り込んでしまったという例がある。SNS 利用がビジネスにおいても浸透している情報管理に対する日頃からの注意喚起、意識づけを行っていくことが重要である。

ウ 執務室及び生産現場の管理

オフィス及び工場においては、物理的管理と技術的管理の両面から対応しなければならない。

(ア) 秘密情報であることの表示

物理的管理としては、秘密情報を含む紙媒体の書面について、「秘密」、「極秘」、「confidential」等のマークを付すことで、当該書面を目にした者が、それが秘密情報であると分かるように表示をすることである。

(イ) 秘密情報を含む書面の管理（持出しの制限）

秘密であることの表示に加えて、当該情報の持出し（社内であると社外であるかを問わず、所定の場所から移動させること）を管理すべきである。当該文書の使用頻度に照らして、たとえば所轄する部署の上司から許可を得ること、文書持出しのための申請書を提出させること、または持出した者が誰であるか分かるよう記録をつけること等が具体的な管理方法として考えられる。また、文書が長期間にわたり持出されたままになってしまわないよう、当日中の返還を義務づけるといったルールも検討すべきである。前記裁判例 No.1-2 (最高裁判所, No. 7769/2557/ CIPITC, TorPor. 98/2551)では、機械部品の製造計画にかかる書面の持出しについて、利用申請書の提出と当日内の返却を義務付けていたことを、秘密管理性を裏付ける事実として認定している。

(ウ) 秘密情報を含む文書の施錠管理

秘密情報を含む書面の保管にあたっては、当該書面を施錠可能なキャビネットで保管したり、金庫において保管したりすることで、同じオフィスや工場で勤務する者であっても、当該文書に容易にアクセスできないよう配慮が必要である。前記裁判例 No.1-2 (最高裁判所, No. 7769/2557/ CIPITC, TorPor. 98/2551)では、顧客情報を含むファイルについて、担当者のみが開けることのできる、施錠されたキャビネットに保管されていたことを、秘密管理性を裏付ける事実として認定している。

(エ) 秘密情報を含む文書の存在するエリアへのアクセス制限

秘密情報が保管されている部屋への立入りを制限したり、警備員を配置したり、入室 ID カードを利用して入退室した者が特定できるように

管理したりすることで、秘密情報に触れる必要のない従業員が物理的にアクセスできないようにする措置も有効である。これは社内の情報遮断という観点からも有効であるほか、次項（オ）で述べる部外者が情報に触れる機会をなくすという観点からも有効である。このような対応が十分にとられていない場合、従業員の誰もが当該秘密情報にアクセスできたとして、秘密管理性が否定される可能性がある。たとえば前記裁判例 No.2-2 (最高裁判所, No. 19015/2555/ CITIPC, Or. 5035/2553)は、製造のための生産ラインが屋外に設置されており、工場に勤務するすべての従業員が生産ラインにアクセス可能であったことや、工場内のどの領域が機密情報で、どの領域がそうでないかを示す標識等は存在しなかったという事実を判断の基礎として、秘密管理性を否定している。

（オ）部外者の情報アクセス制限

生産現場においては、取引先候補、外部業者、見学者の訪問を受ける場合もある。すると、生産現場の従業員においてのみ共有している情報が、部外者に漏れてしまう可能性がある。こういった者が営業秘密となる秘密情報に触れないよう、秘密情報が存在するエリアへは立ち入ることができないようにすること、入館者記録をとること、訪問中はバッジやカードを付けて部外者であるとわかるようにしておくこと、といった対応が考えられる。

エ ライセンシー等外部事業者の管理

社内における営業秘密の取扱いのみでなく、社外に対して営業秘密を提示する場合にも注意が必要である。情報は、ひとたび社外に出てしまえば、その流通をコントロールすることは著しく困難になるからである。

原則としては、①営業秘密を開示する可能性のある第三者との間では必ず秘密保持契約を締結すること、②秘密保持契約を締結するまでは営業秘密を開示しないこと、③相手方に守秘義務を課している場合であっても、相手方に共有する必要のない情報をむやみに渡さないことが基本的な方針となる。

前記裁判例 No.2-2 (最高裁判所, No. 19015/2555/ CITIPC, Or. 5035/2553)においては、金型の製造業者に対して、秘密保持契約を締結することなく金型に関する情報を提供していたとして、当該金型に関する情報の秘匿性が失われていたとの認定がなされているから、注意が必要である。

（コラム）テレワーク時における情報セキュリティ上の留意点

近時、新型コロナウイルス（COVID-19）の流行を契機として、タイでもテレワークを推奨する企業が増えている。テレワークを実施する際には、会社の情報が社外に漏れることがないように、より一層の注意が必要となる。具体的な留意事項として、①BYOD

(Bring Your Own Device)導入、②在宅勤務のための情報持ち出し、及び③Web 会議の実施の場面で、それぞれ情報管理について注意すべきである。

- ①BYOD (Bring Your Own Device)とは、従業員個人が保有する PC や携帯電話端末を業務に利用することを意味する用語である。会社にとっては、個々人のデバイスを購入しなくてよい点で経済的であり、また、新型コロナウイルスの影響による急なテレワーク移行に伴って、個々人に支給する PC や携帯電話端末を調達する時間的余裕がない中で BYOD を選択した企業も多いようである。BYOD のリスクは、前記コラム「SNS 利用の制限について」で述べたところと基本的に共通している。すなわち、(i)セキュリティの弱さ、(ii)トラッキング・モニタリングの困難さ、(iii)紛失・盗難リスク、(iv)退社後に情報を保有し続けてしまうこと、が挙げられる。
- ②在宅勤務のための情報持ち出しについては、テレワーク体制が十分に整備されていない場合などに、会社の資料を印刷して自宅に持ち帰ったり、必要な情報を USB フラッシュメモリに保存して持ち帰ったりして、自宅で業務を行うことにより、紛失・盗難による情報漏えいのリスクが高まるほか、情報の管理が行き届かなくなる点が挙げられる。
- ③Web 会議については、国外との往来が困難になったことや、人と人との接触を減らす趣旨から、タイにおいても利用が急速に進んでいる。Web 会議における情報管理上の注意点としては、Web 会議システムそのもののセキュリティ上のリスクがある他に、画面内に不必要な情報が映り込んでしまうことが挙げられる。特に Web 会議システムの画面共有システムを利用する際に、画面操作を誤って不必要な情報を会議参加者全員に共有してしまうといった例がしばしば発生する。Web 会議導入期における、特に利用者が操作に不慣れなために発生する事象ともとらえられるが、自社情報や、他社の秘密情報を不注意で漏らしてしまうことがないよう、細心の注意を心掛けるべきである。

(4) タイにおいて特に気を付けるべきポイント

ここまでタイにおける営業秘密管理の具体的な対策を述べてきたが、その具体的な方法は、日本におけるそれと大きく異なるものではない。日本であれタイであれ、ステップ 1 から 3 を通じて、会社が保護すべき情報類型を認識し、それを保護するためのルールを策定したうえで、運用するという大きな方針や対応に違いはない。そのうえで、日系企業がタイにおいて気を付けなければならない点としては、日本本社における営業秘密管理規程等を、そっくりそのままタイ現地法人で展開することには適さない場合も多いことである。たしかに、日本とタイとの営業秘密保護に関する制度は似通っているところも多いのであるが、情報管理はタイ現地における情報取得と利用の実態、及び現地法人の人的資源や組織構成に則って検討される必要がある。秘密とすべき情報類型にも差があるであろうし、また前記コラム「SNS

利用の制限について」で述べたような実務慣行の違いもある。日本本社の情報管理体制は大いに参考にされるべきであるが、現地での実務慣行や現地役員等の意見も踏まえて、実効的な情報管理体制を構築しなければならない。

2 関連契約書作成上の留意点

前記「1 タイにおける営業秘密管理の3ステップ」を実装するうえで中心となる関連文書は、以下のものがあげられる。

- ①社内における営業秘密の取扱いに関する包括的ルールを定める「営業秘密管理規程」
- ②従業員に対して守秘義務を課すための「就業規則」「雇用契約」及び「秘密保持誓約書」
- ③取引先等第三者に対して守秘義務を課すための「秘密保持契約」

以下には作成の留意点について簡潔に述べるが、具体的な規定案については第3章も参照のこと。

(1) 社内規程の策定

会社において営業秘密を所轄する部署や役職の規定と、会社が秘密情報として取扱う情報の類型及びその具体的な管理方法について規定すべきである。情報の類型によって、より厳密な管理が求められるものと、ある程度ゆるやかに取扱わざるをえないものがあるであろうから、たとえばランク A 情報とランク B 情報などと二類型に分けて取扱い方法を記載することも可能である。

(2) 従業員の秘密保持義務

ア 就業規則

就業規則制定にあたって特に留意すべきことは、①退職後の秘密保持義務についても明記することと、②懲戒規定を設けることである。

タイにおいては、従業員数が10名以上のすべての会社に、タイ語での就業規則の策定が義務付けられている。このため、就業規則において秘密保持義務を規定することによって、会社に所属するすべての従業員に対して守秘義務を課すことができ、違反時のペナルティ（懲戒）も可能となる。ただし、原則としてすべての従業員に対して同列の画一的な義務を課ことになるから、個々の従業員の職務や役職に応じた対象情報の絞り込みや、守秘義務の年数調整（過度に長期にわたる守秘義務は無効と判断される可能性がある）は難しい。したがって、このような個別対応は、雇用契約または秘密保持誓約書を通じて行うべきこととなる。

イ 雇用契約

個々の従業員との間で締結する雇用契約においても、守秘義務を課すことを明記しておくべきである。特にマネージャークラスの従業員に対して、就業規

則で定める以上の守秘義務を課すような場合には、雇用契約の中で規定することになる。

また、営業秘密と直接関係するわけではないものの、退職後の一定期間同種の職業に就くことを禁じる競業避止義務についても検討すべきである。実際の営業秘密侵害の多くは、会社の従業員が競業他社に転職したり、自ら同種の事業を営む会社を設立したりすることによって生じている。このような事態を防ぐ方法として、競業避止義務を課すことは非常に有効である。特にマネージャークラス以上の従業員や役員との契約において検討されたい。

なお、タイにおいても競業避止義務は無制限に有効と認められるわけではないものの、対象となる事業の範囲と期間が、当該従業員が従事していた業務内容、役職、または支払われていた賃金に比して合理的な範囲内といえる範囲で許容される。経済補償金の支払いは、必須の要件ではないものの考慮要素の一つとなりうるから、役員に対して長期の競業避止義務を課すような場合には、経済補償金の支払いも検討するべきであろう。

ウ 秘密保持誓約書

上記「イ 雇用契約」については入社時に締結することが想定されるが、入社時以降においても、配転時、退職時、秘匿性の高いプロジェクトへの参入時等のタイミングにおいて、それぞれ従業員から秘密保持誓約書を提出させるべきである。

特に営業秘密漏えい事件の多くが従業員の退職後に起こることを考慮すると、退職時に秘密保持誓約書を取得しておくことは非常に有効であると考えられる。もっとも、退職時に秘密保持誓約書を差し入れさせることは容易でない場合もある。とりわけ従業員が非友好的なかたちで退職を決めたような場合には、会社から秘密保持誓約書を差し入れるよう求めても、これに応じない可能性が高い。だからこそ退職時秘密保持誓約書の有効性は強い（従業員の任意の同意であると認定されやすい）と考えられているのであるが、退職時の秘密保持誓約書提出を強制できない場合があることも想定して、就業規則、雇用契約書、秘密保持誓約書と三段階の構えで従業員に守秘義務を課す体制とすることが適切である。

(3) 取引先等第三者の秘密保持義務

企業間であらたに営業秘密が開示される場面においては、かならず秘密保持契約を締結すべきである。具体的な場面としては、M&A やそれに先立つデューデリジェンスの実施時、共同開発事業の検討開始時、製造に関する成分配合、図面、金型等を提示して製造委託を行う場合等が想定される。

秘密保持契約の内容としては、秘密保持の対象となる情報の特定、第三者に対す

る開示の禁止、秘密情報の管理方法及び目的外利用の禁止、秘密情報の破棄・返還に関するルール等を規定することが一般的である。

3 漏えい事案への対応

会社の営業秘密が漏えいしたことを認識した場合には、可及的速やかに原因究明と被害拡大防止の措置を取らなければならない。具体的な対応策としては、以下(1)から(4)の対応を行う必要がある。

(1) 初期調査の実施

会社の営業秘密がどこから漏えいしたのか、早急に原因究明を行わなければならない。情報漏えいの態様は様々であり、初期調査の方針も一概に述べることは難しいのであるが、一般的には漏えいした情報の性質に照らして漏えい主体の特定を検討する。具体的には、①従業員、②退職した元従業員、③取引先、④その他外部の第三者のいずれによる情報漏えいであるのかを究明する。秘密情報に対するアクセス制限が機能していれば、漏えいした情報の内容から、漏えい主体の絞り込みが可能な場合もあるだろう。

次に、情報漏えいのルート（手段）について調査を行う。たとえば従業員による漏えいの場合であれば、紙媒体の資料を持出したのか、Eメール等で部外者へ情報を送っていたのか、等具体的な行為態様を特定していく。ただし、これは調査方法の一例に過ぎず、事案の性質によっては、漏えいルートが先に判明し、そこから漏洩主体を絞り込んでいく場合もあるだろう。

これらの初期調査を通じて早急に確認すべき事項としては、(i)漏えいした情報の範囲、(ii)漏えいの原因（主体と手段）、(iii)漏えいが現在も続いているのか、または今後も続く可能性があるのか、(iv)当該漏えいによって誰が営業秘密を得たのか、といった事実である。

(2) 被害拡大の防止と証拠の保全

情報漏えいを認識した時点でまだ漏えいが続いている場合には、早急に情報の漏えいを止めなければならない。また、次項「(3) 捜査機関との連携と法的手続き」に述べる権利行使を見据えて、証拠保全も早期に行うべきである。「被害拡大防止」と「証拠保全」の二点は、可能な限り迅速に実施するべきである。なぜなら、一度漏えいしてしまった情報を取り戻すことは困難であるし、時間が経つとともに得られる証拠は少なくなっていくからである。

被害拡大防止の観点からは、情報漏えい先に対して警告書を送付することが考えられる。警告書受領以降の情報開示や情報受領が、営業秘密の侵害行為に該当しうることを認識させ、さらなる被害拡大を防止することができる場合があるためである。

また、証拠保全の観点からは、弁護士等の外部専門家に依頼して、関係当事者へのヒアリングを実施したり、フォレンジックベンダ等の専門業者に依頼して、PCやデータサーバーのフォレンジック調査を実施したりしておくことが好ましい。なお、タイにおいても複数の事業者がフォレンジックサービスを提供しており、情報漏えいの調査や証拠保全を行ううえでは有効な手段であるといえることができる。もっとも、フォレンジック対象を無限定に広げてしまうと費用も高額になってしまうため、実務上はフォレンジックの対象となるサーバーや端末を限定して実施する場合も多いと思われる。この際、的確な範囲画定を行うためにも、どのような情報がどの端末に保管されているのか、どの範囲の社員がアクセス可能であるかということ、会社としてあらかじめ把握しておくべきである。

(3) 捜査機関との連携と法的手続き

第1章「4 営業秘密侵害に対する救済手段」で述べた各種権利行使を検討することとなる。刑事事件性がある場合、すなわち営業秘密の公表によって、当該情報の営業秘密性が失われたと認められ、法33条違反の可能性がある場合には、警察の助力を得られる可能性があるから、可能な限り警察と連携して捜査を進めるべきである。そのうえで、刑事告訴、民事訴訟の提起を検討していくこととなる。なお、営業秘密侵害罪にかかる刑事的措置の告訴期間は、被疑事実と被疑者を知った日から3か月とであるから、調査資料や説明資料を整えて警察に届け出るまでの時間はきわめて短い。迅速に対応を行う必要がある。

(4) 再発防止策の策定

(1)から(3)までの対応を行い、漏えい事案がひと段落したら、あらためて原因を明らかにしたうえで、再発防止策を検討し、実施していくべきである。

なお、日系企業においては、不正行為を行った従業員や元従業員への処罰をためらう場合も多いが、不正行為に対しては刑事告訴、民事訴訟の提起を含めて毅然とした態度で臨まなければ、類似の案件を誘発することになりかねない。会社として、いかなる不正行為に対しても厳然と対処していく姿勢を見せることで、社内不正に対する抑止力とし、もってコンプライアンス体制の強化と再発防止につとめるべきである。

第3章 各種関連書類参考書式（フォーム）

1 雇用契約における一般的な守秘義務条項例

Article []. Confidentiality

The Employee agrees to use Confidential Information only to carry out his/her duties pursuant to the employment agreement. The Employee also agrees not to use the Confidential Information for his/her own benefit or the benefit of any person, corporation, or entity other than the Company while employed by the Company and after termination of his/her employment or this agreement and shall not disclose or supply any such Confidential Information to any third party at any time without the prior written consent of the Company.

Unless otherwise provided by the Company, in the event the Employee is required to disclose Confidential Information to other Employees under the Employee's direction, the Employee shall limit the access of such other Employees to Confidential Information on a strictly need-to-know basis and shall cause such other Employees to keep Confidential Information confidential.

The Employee shall at all times keep the Confidential Information of the Company confidential in the manner prescribed by the Company in this agreement and any internal policy.

2 従業員と締結する営業秘密に関する秘密保持契約の条項例

Article []. Definition

“Trade Secrets” means any trade information that is commercially valuable to the Company and not generally known or accessible by persons who are normally connected with the information pursuant to the Trade Secrets Act of Thailand. For the avoidance of doubt, Trade Secrets shall be deemed a part of the Confidential Information.

Article []. Protection of Trade Secrets

Item [] The Company may notify, label, or otherwise identify any information that is considered to be a Trade Secret as “Strictly Confidential” or another similar term. The Company may appoint or entrust any person to protect the Trade Secrets of the Company (“Authorized Person”).

Item [] In the event the Company identifies any information as a Trade Secret, the Employee agrees to comply with the strictest measures to maintain the confidentiality of such Trade Secret in the manner specified by the Company, in addition to the following:

- (a) Except where the Employee is permitted to access Trade Secrets under the Company’s internal rules, the Employee shall not access Trade Secrets without written permission from the Company or the Authorized Person. In the event that the Company grants such permission, the Employee shall present such permit to the Authorized Person.
- (b) The Employee shall return Trade Secrets, including any copies thereof, to its set location before the Employee leaves the office each day. The Employee shall not take any files or materials containing Trade Secrets out of the Company site(s), unless explicitly permitted by the Company or the Authorized Person.
- (c) The Employee shall not make any copy of, share, or distribute Trade Secrets (whether in hard copy or by electronic means) unless permitted by the Company or the Authorized Person.
- (d) If the Employee accesses Trade Secrets via electronic means, the Employee shall not disclose any username(s) and passcode(s) authorizing access to such Trade Secrets to any persons.
- (e) [If the Employee is acting as an Authorized Person, the Employee shall ensure that Trade Secrets are kept independently and separately from the other Confidential Information of the Company and any other information. At minimum:
 - (i) Hard copies of Trade Secrets shall be stored in secured cabinets accessed by locks and keys, and the keys shall be kept in a separate secured location; and
 - (ii) Electronic copies of Trade Secrets shall be stored in secured files or software on a

secured computer, all of which can be accessed by username(s) and passcode(s) provided by the Company or the Authorized Person, and such username(s) and passcode(s) be regularly updated.]

- (f) The Employee shall regularly check the files or programs to ensure that Trade Secrets are properly maintained and have not been lost or stolen. [Where Trade Secrets are returned, the Authorized Person shall confirm that such Trade Secrets have been duly returned. The Authorized Person shall maintain a record of the access dates and times, return dates and times, signatures of the persons that have accessed Trade Secrets, and confirmations that the Trade Secrets have been returned as is.]

Item [] In the event the Employee discovers any Trade Secrets of the Company, whether by way of reverse engineering of the Company's products or otherwise, the Employee agrees that the information obtained from such discovery shall be the property of the Company and shall form a part of the Confidential Information (including Trade Secrets) pursuant to this Agreement.

Article []. Non-Competition

The Employee agrees, during the term of his/her employment with the Company [and for [one (1) year] from the date of termination of his/her employment with the Company], not to engage in any other employment, occupation, consulting, or other business activity similar to, the same as, or in competition with the business of the Company or to engage in any other activities that conflict with its duties toward the Company.

3 取引先等第三者と締結する営業秘密に関する秘密保持契約条項例

Article []. Definition

“Trade Secrets” means any trade information that is commercially valuable to the Disclosing Party and not generally known or accessible by persons who are normally connected with the information pursuant to the Trade Secrets Act of Thailand. For the avoidance of doubt, Trade Secrets shall be deemed a part of the Confidential Information.

Article []. Protection of Trade Secrets

Item [] In the event that the disclosing party (“Disclosing Party”) would like the receiving party (“Receiving Party”), including its Authorized Representatives (as specified below), to take appropriate measures to keep confidential the Trade Secrets of the Disclosing Party [and/or its [Representatives]] pursuant to this Article, the Disclosing Party shall notify, label, or otherwise identify that such information is a Trade Secret.

Item [] Subject to Paragraph 1 of this Article, the Disclosing Party may label or otherwise identify an information that is considered to be a Trade Secret as “Strictly Confidential” or another similar term. If specified by the Disclosing Party, the Receiving Party shall limit access to such Trade Secrets only to those identified as Authorized Representatives. If requested by the Disclosing Party, the Receiving Party shall cause the Authorized Representatives to enter into a written non-disclosure agreement with the Disclosing Party separate from this Agreement.

Item [] The Receiving Party, including its Authorized Representatives, shall comply with the strictest measures to maintain the confidentiality of the Trade Secrets of the Disclosing Party [and/or its [Representatives]] in the manners specified by the Disclosing Party, including the following:

- (a) Trade Secrets shall be stored in their original format or files (whether as hard copies or in electronic form), and such format or files shall be kept separately from other Confidential Information or any other information of the Receiving Party;
- (b) Hard copies of Trade Secrets shall be stored in secured cabinets accessed by locks and keys, and the keys shall be kept in a separate secured location;
- (c) Electronic copies of Trade Secrets shall be stored in secured files or software on a secured computer, all of which can be accessed by username(s) and passcode(s). The Receiving Party shall not disclose the username(s) and passcode(s) to any persons other than the Authorized

Representatives;

- (d) The Receiving Party and its Authorized Representatives shall not make any copy of, share, or distribute Trade Secrets to any persons except in the event that the written consent of the Disclosing Party therefor is acquired;
- (e) The Receiving Party shall maintain a record of access to the Trade Secrets and, if requested by the Disclosing Party, shall send such record to the Disclosing Party without undue delay; and
- (f) If requested by the Disclosing Party, the Receiving Party shall provide a letter certifying that Trade Secrets, including any authorized copies thereof, are kept in the format and files as originally provided by the Disclosing Party.

Item [] The Receiving Party [and/or its [Representatives]] shall not perform any action that constitutes reverse engineering of any products of the Disclosing Party [and/or its [Representatives]], and such reverse engineering action shall be deemed a violation of this Agreement. In all events, the information obtained from reverse engineering shall be the property of the Disclosing Party or its Representative(s) and shall form a part of the Confidential Information (including Trade Secrets) pursuant to this Agreement.

経済産業省委託事業

タイにおける営業秘密管理マニュアル作成

2021 年 3 月

禁無断転載

[調査受託]

TMI Associates (Thailand) Co., Ltd.

独立行政法人 日本貿易振興機構

バンコク事務所

(知的財産権部)

本冊子は、2020年度に日本貿易振興機構バンコク事務所知的財産部が調査委託を行ったTMI Associates (Thailand) Co., Ltd.が作成した調査報告等に基づくものであり、その後の法改正等によって記載内容の情報は変わる場合があります。また、記載された内容には正確を期しているものの、完全に正確なものであると保証するものではありません。

Copyright(C) 2020 METI/JETRO. All right reserved.