

経済産業省委託

令和2年度重要技術管理体制強化事業（中小企業アウトリーチ事業（営業秘密漏えい対策））

2021年3月

独立行政法人 日本貿易振興機構

イノベーション・知的財産部

目次

[1] はじめに.....	2
[2] 個別支援.....	3
1. 概観.....	3
2. 個別支援企業.....	3
3. 個別支援企業へのアンケート結果	4
[3] 普及啓発.....	6
1. 概観.....	6
2. 個別支援企業募集セミナー	6
(1) 日本	6
(2) 中国	6
3. 成果普及セミナー.....	6
4. 技術流出防止管理説明会	6
[4] マニュアル作成.....	8
1. 概観.....	8

〔1〕はじめに

グローバル化により海外に進出する日系企業が増加し、それに伴い技術情報等の漏洩リスクも増大している。平成 29 年度の「企業における営業秘密管理に関する実態調査」では、約 9 割の企業が「営業秘密の漏えいリスクが高まっていると感じる」と回答した。過去 5 年間で漏えいがあったと回答した企業の約 1 割が外国の競業企業に漏えいしたと回答しており、海外での漏えいを防ぐ管理体制の整備が必要となっている。

一方、中小企業を中心に、海外拠点におけるリソースは限定されており、営業秘密管理の重要性認識や管理体制整備が不十分な企業は少なくない。営業管理の重要性が認識されていない場合、競合他社の立ち上げ等自社ビジネスへの影響が出て初めて対応策を検討することになるが、既に流出してしまった秘密情報は取り戻すことができない。また、重要性を認識している場合でも、製造や労務管理等に忙殺され、管理体制整備にまで手が回らないケースも散見される。

そこで、本事業では、在外日系中堅・中小企業を主なターゲットにすえ、専門家によるハンズオン支援と情報提供・普及啓発活動による意識の底上げを通じて、これまでに蓄積した営業秘密漏えい事案に関する知見等を活用しながら、日本企業の営業秘密管理体制整備の支援を拡充させ、海外での技術・ノウハウの意図せぬ流出を防ぐことを目的として各種事業を実施した。

〔２〕 個別支援

１．概観

中国に進出する日系企業は、32,000 社超と世界最多であるが、人材の流動性が高く、営業秘密流出に関する相談も多いことから、引き続き、本事業へのニーズが見込まれたため、昨年度より継続して中国を実施対象とした。また、近年、ASEANに進出する日系企業が増加しており、外務省の海外進出日系企業拠点数調査（平成30年）によれば、日系企業の拠点数上位10ヶ国中5ヶ国をASEANが占めており、タイに進出する日系企業は3,925社、ベトナムに進出する日系企業は1,816社となっていることに加え、JETROが実施した日本企業の海外事業展開に関するアンケート調査（令和元年度）によれば、今後海外で事業拡大を図る国として、中国に次いでベトナム、タイがあげられていたことから、ベトナム、タイを本事業の実施対象とした。具体的には、営業秘密管理体制整備を希望する在中国日系企業26社、在タイ日系企業6社、在ベトナム日系企業1社に対し、現地の専門家により営業秘密管理状況のヒアリングを実施し、アドバイス（管理状況の改善、契約書等の改正案作成）、必要に応じて現場確認や従業員や管理職への研修等を行った。

２．個別支援企業

（１）中国

	企業	支援先拠点	支援期間
1	A社	北京	5月13日(水)～1月26日(火)
2	B社	上海	7月30日(木)～1月22日(水)
3	C社	上海	7月28日(火)～1月26日(火)
4	D社	吉林省	7月21日(火)～1月20日(水)
5	E社	遼寧省	10月15日(木)～1月26日(火)
6	F社	江蘇省	7月22日(水)～11月27日(金)
7	G社	広東省	8月7日(金)～1月6日(水)
8	H社	遼寧省	8月19日(水)
9	I社	広東省	8月26日(水)～1月6日(水)
10	J社	広東省	9月1日(火)～1月6日(水)
11	K社	上海	10月12日(月)～1月12日(火)
12	L社	江蘇省	11月20日(月)～1月29日(金)
13	M社	上海	10月20日(火)～12月7日(月)
14	N社	北京	10月19日(月)～1月28日(木)
15	O社	遼寧省	10月21日(水)～1月28日(木)
16	P社	上海	11月25日(水)～1月
17	Q社	遼寧省	11月2日(月)～1月20日(水)

18	R 社	遼寧省	12 月 10 日(木)～1 月 28 日(木)
19	S 社	上海	12 月 9 日(水)～1 月 29 日(金)
20	T 社	上海	11 月 30 日(月)～1 月 29 日(金)
21	U 社	上海	1 月 15 日(金)～1 月 29 日(金)
22	V 社	広東省	12 月 18 日(金)～1 月 29 日(木)
23	W 社	江蘇省	12 月 15 日(火)～1 月 29 日(金)
24	X 社	江蘇省	12 月 25 日(金)～1 月 26 日(火)
25	Y 社	江蘇省	12 月 22 日(火)～1 月 18 日(月)
26	Z 社	上海	12 月 4 日(金)～1 月 26 日(火)

(2) タイ

	企業	支援先拠点	支援期間
1	AA 社	バンコク	10 月 12 日(月)～2 月 25 日(木)
2	AB 社	バンコク	10 月 9 日(金)～2 月 19 日(金)
3	AC 社	バンコク	10 月 6 日(火)～2 月 22 日(月)
4	AD 社	バンコク	10 月 12 日(月)～2 月 24 日(水)
5	AE 社	サムットプラーカーン県	10 月 14 日(水)～2 月 25 日(木)
6	AF 社	バンコク	10 月 14 日(水)～2 月 23 日(火)

(3) ベトナム

	企業	支援先拠点	支援期間
1	AG 社	ドンナイ省	8 月 25 日(火)～2 月 23 日(火)

3. 個別支援企業へのアンケート結果

アンケート回答企業 29 社中、20 社で営業秘密漏えい防止策を導入。

	企業	導入済みもしくは導入が決まっている対策
1	A 社	・日本語および中国語による秘密保持規制及び秘密保持契約の作成と締結。 ・各部門における秘密保持実施細則の作成
2	B 社	・全部署での営業秘密管理台帳の作成
3	F 社	・携帯電話の持ち込み禁止
4	M 社	・取引先との契約書における条項の追加。
5	O 社	・新しい契約書の導入

6	P 社	・社員に対する機密保持契約の見直し
7	Q 社	・機密内容のリスト化、機密管理規定の修正
8	R 社	・従業員に対する秘密漏えいに係る誓約書の取り交わし
9	S 社	・社内規程の更新
10	T 社	・プリンター印刷時の社員カードの照合
11	V 社	・営業秘密情報の特定と識別、施錠、持ち出し管理
12	W 社	・中国 OEM 先との契約書の機密保持条項に、自社からの開示情報の管理状況を監査する規定を追加
13	X 社	・規程や契約書の改善
14	Y 社	リーガルチェックされた書類の利用
15	Z 社	・書類、会社関連規定の更新
16	AA 社	・顧客との NDA の雛型
17	AB 社	・採用時の情報管理順守契約 ・管理情報の分類と管理者の設定・運用
18	AC 社	・新規雇用時に、その従業員との秘密保持契約の締結
19	AE 社	・新規雇用契約書への秘密情報に関する記述を追加 ・営業秘密管理規定の作成
20	AG 社	・情報管理規定の制定と周知

〔3〕普及啓発

1. 概観

営業秘密管理体制のモデルケースや流出事例、過去の支援利用企業の事例を紹介し、営業秘密管理の重要性について啓発するとともに、個別支援のニーズを掘り起こすことを目的として、企業関係者に対しセミナーを行った。また、技術流出防止管理説明会に講師を派遣した。

2. 個別支援企業募集セミナー

専門家より、中国における営業秘密漏えい対策について講演を行うとともに、ジェトロ職員から営業秘密漏えい対策支援事業について紹介する WEB セミナーを日本国内（東京）及び中国（上海）で開催した。

（1）日本

- ・ 実施日時 2020 年 8 月 21 日（金）14：00～16：00
開催形式 WEB セミナー
参加人数 317 名

（2）中国

- ・ 実施日時 2020 年 7 月 2 日（木）14：30～16：00
開催形式 WEB セミナー
参加者数 150 名

3. 成果普及セミナー

中国、タイ、ベトナムそれぞれの専門家より、営業秘密漏えい対策について講演を行う WEB セミナーを日本国内（東京）で開催した。

- ・ 実施日時 2021 年 2 月 19 日（金）14：00～16：30
開催形式 WEB セミナー
参加人数 168 名

4. 技術流出防止管理説明会

ジェトロ職員を派遣し、営業秘密保護及び技術流出防止のための対策について講演を事前収録し、技術流出防止管理説明会において当該講演動画の配信を行なった。

- ・ 実施日時 2020 年 7 月 29 日（水）、8 月 5 日（水）、8 月 19 日（水）、9 月 2 日（水）、9 月 7 日（月）、9 月 16 日（水）、10 月 2 日（金）、10 月 12 日（月）、10 月 14 日（水）、10 月 16 日（金）、10 月 26 日（月）、11 月 6 日（金）、11 月 11 日（水）、11 月 13 日（金）、11 月 17 日（火）、11 月 27 日（金）、12 月 16 日（水）、

2021 年 1 月 14 日 (木)、1 月 15 日 (金)、1 月 26 日 (火)、1 月 29 日 (金)、
2 月 12 日 (金)

開催形式 WEB セミナー

[4] マニュアル作成

1. 概観

タイ、ベトナム、シンガポールについて、関係法令における営業秘密の定義・対象範囲、営業秘密の流出事例、営業秘密の判例・紛争事例、営業秘密の保護・管理上で特に気を付けるべきポイント、参考となる資料（各種ひな形等）の情報収集をし、タイ、ベトナムについては「営業秘密管理マニュアル」を作成した（別紙参照）。

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）

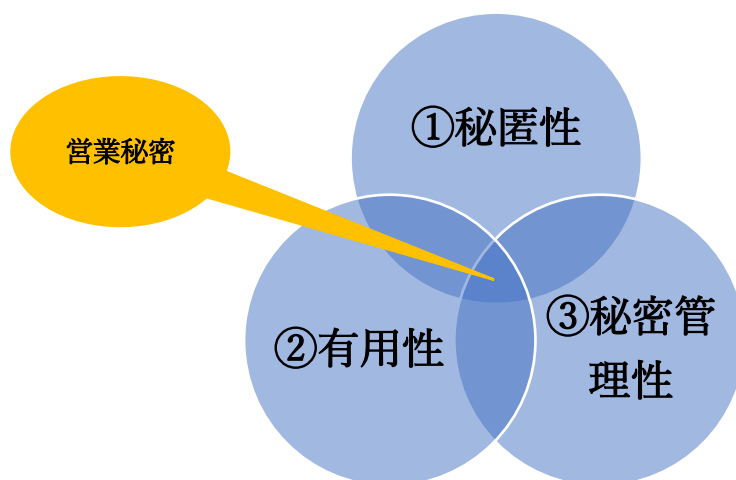
ア 農薬製品の登録に関連する規則

- ・ 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ってしまうと、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しており、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、会社のメールアドレスから個人のメールアドレスに送信することが、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ドレスに送信することは、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ドレス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ドレス及び私用 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。

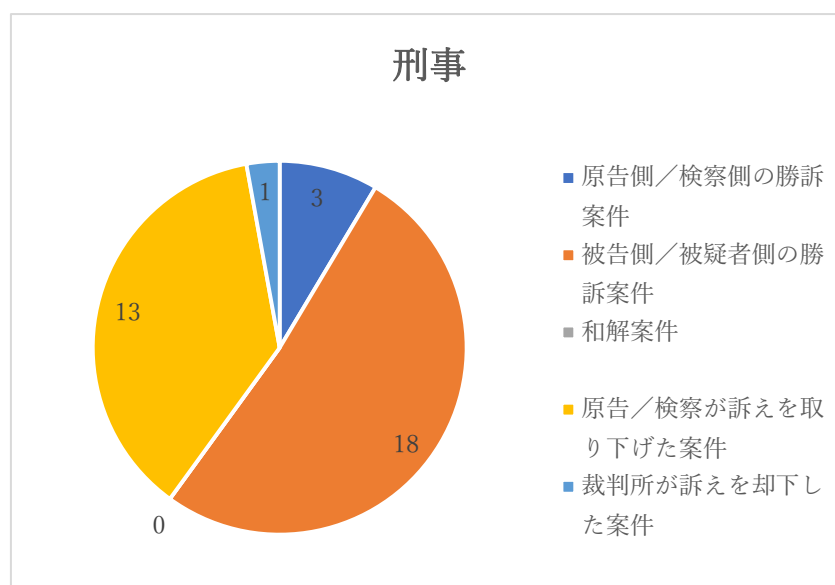
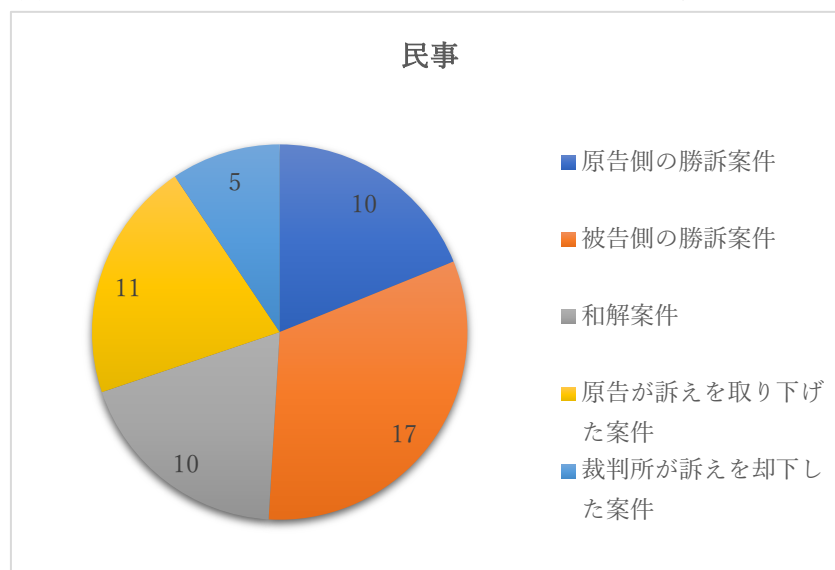
次に、営業秘密侵害の場合には、証拠収集の方法としてインカメラ手続きが利用可能であるメリットも大きい。営業秘密は、秘密であることによって価値を生じる情報なのであるから、裁判によってその内容が公開されてしまえば本末転倒になってしまう場合がありうる。また、情報漏えいの案件においては、情報が漏えいしたことによる損害額を立証することは非常に困難であるが、本法の適用を受けることで、損害賠償額を裁判所が適切と考える金額で認定してしまうことによる立証負担の軽減や、場合によっては（日本とは異なり）懲罰的損害賠償が認められることによる利益も大きい。

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の製造していた。
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.

経済産業省委託事業

ベトナム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
ハノイ事務所

目 次

はじめに	1
第 1 章 ー法制度編ー	2
1. ベトナムにおける営業秘密の定義	2
(1) 法律上の 3 つの要件	2
(2) 営業秘密の例外	3
2. ベトナムにおける営業秘密所有者の権利	4
(1) 営業秘密所有者	4
(2) 営業秘密所有者の権利	4
3. ベトナムにおける営業秘密侵害行為の定義	5
(1) 知的財産法上の定義	5
(2) 競争法、サイバーセキュリティ法における営業秘密侵害行為	9
4. ベトナムにおける営業秘密侵害の実態	11
(1) ベトナムにおける営業秘密侵害の 3 つのパターン	11
(2) 従業員漏えい型	11
(3) 取引先漏えい型	13
(4) 第三者不正取得型	14
(5) 新たな侵害形態	14
5. 営業秘密侵害に対する法的措置	15
(1) 民事的救済	17
(2) 行政措置	19
6. 営業秘密に関する法規制の改正状況	19
7. 営業秘密規定の域外適用	22
8. 裁判例	23
第 2 章 ー営業秘密漏えい対策実践編ー	24
1. 総論	24
(1) 管理体制の構築を考える上での 2 つの視点	24
(2) 漏えい対策実効性の観点からの管理体制の構築	24
2. 管理体制整備のステップ 1ー管理体制の現状の確認	26
(1) 現状把握の必要性	26
(2) セルフチェックシート	26
3. 管理体制整備のステップ 2ー営業秘密情報の洗い出し及び重要度の区分	29
(1) 営業秘密情報の洗い出し（☞ハンドブック P.6～13）	29
(2) 重要度の区分（☞ハンドブック P.14～16）	30

(3) 特許.....	30
4. 管理体制整備のステップ3ー管理体制の整備.....	31
(1) 担当部門/担当者の設置（☞ハンドブック P.95～106）	31
(2) 従業員の管理	32
(3) 執務室の管理	40
(4) 生産現場の管理.....	41
(5) 取引先の管理	43
5. 漏えい時の対応	45
(1) 漏えいの兆候（☞ハンドブック P.122～127）	45
(2) 初動対応(☞ハンドブック P.127～130)	47
(3) 民事訴訟.....	47
(4) 行政措置.....	48
(5) 冒認出願の確認.....	49
(6) 対応フロー	49
参考書式.....	51
1. 就業規則における秘密保護関連規定の例	51
2. 従業員の秘密保持に関する誓約書の例.....	60
3. 退職時の秘密保持に関する誓約書の例.....	64
4. 取引先との秘密保持契約書の例	69
5. 来訪者受付表（ベトナム語/日本語併記）	79

はじめに

市場において、自社製品・サービスが競争力を発揮するためには、それらを支える自社独自の技術情報や営業情報といった営業秘密を適切に保護することは極めて重要であり、製造、販売等の拠点を海外にも有する場合には、各国における関連法規や権利行使のプラクティス、商習慣等の相違を考慮した上で、拠点ごとに営業秘密を適切に管理する必要がある。

とりわけ、ベトナムでは、人材流動性の高さや営業秘密を含む知的財産権保護に対する社会的意識が十分に成熟していないこと等を背景として、営業秘密の保有者が意図しない漏えいや流出が多く発生しており、日系企業の中には被害の実例も存在しているにもかかわらず、ベトナム拠点での営業秘密管理体制の整備が手付かずのままとなっているものも少なくない。

そこで、本稿は、こうした実情を踏まえ、日系企業のベトナムにおける営業秘密管理体制の整備・構築、又はその見直しに資するべく、ベトナムにおける裁判例やプラクティス、営業秘密支援事業¹における日系企業の改善事例や筆者らの経験も踏まえて、基本マニュアルとしてまとめたものである。

本稿は、「法制度編」と「漏えい対策実践編」から構成され、いずれのパートについても、日本との異同や日本との比較において、ベトナムで特に留意すべき点を中心に説明している。もともと、具体的な管理手法等をはじめとして、日本における営業秘密管理の考え方と共通する部分も多く、経済産業省の「秘密情報の保護ハンドブック～企業価値向上に向けて～」²（以下、本稿では「ハンドブック」という。）の内容が参考になると考えられるため、本稿では、一部、ハンドブックの記載を引用し、また、ハンドブックの参照箇所を明記している。ハンドブックは、営業秘密管理の基本的な考え方を網羅しており、本稿とあわせて活用することで、ぜひ、ベトナムにおける営業秘密の管理の整備にお役立て頂きたい。

¹ JETRO が、在ベトナム日系企業の営業秘密管理体制の構築を支援する事業（https://www.jetro.go.jp/services/ip_service_prevent.html）[最終アクセス日：2020年11月18日]。本稿では、「支援事業」という。なお、募集の有無や内容等は、年度により変更される可能性があるため、詳細はJETRO ホームページにて随時確認されたい。

² <https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf> [最終アクセス日：2020年11月18日]

第1章 一法制度編一

1. ベトナムにおける営業秘密の定義

(1) 法律上の3つの要件

一般に、「営業秘密」というと、工場内で用いられる製造ノウハウ等が想起されやすい。しかし、法律上は、営業秘密はかかる技術情報に限られないし、また、逆に、企業が保有している技術情報のすべてが法律上「営業秘密」として保護されるわけではなく、法律上の「営業秘密」の定義を構成する要件を満たす必要がある。

いわゆる「営業秘密」の保護については、国際的には、WTO・TRIPs 協定（知的財産権の貿易関連側面協定）において規定されており³、日本やベトナムなどを含む WTO 加盟国は、営業秘密の保護について国内法を整備する必要がある。このため、ベトナムにおける営業秘密の定義は、日本とよく似ている。

日本の不正競争防止法では、営業秘密は、「秘密として管理されている生産方法、販売方法その他事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの」と定義されている（第2条第6項）。

一方、ベトナムでは、営業秘密の保護等は、知的財産法⁴に規定されている。同法では、営業秘密は、「財政的投資・知的投資から得られた情報であって、開示されておらず、かつ、事業において利用可能な情報」と定義されている（第4条第23項）。そして、営業秘密は以下の要件を満たす場合に（法令上の）保護を受けると定めている（第84条）。

- (i) 公知でなくまた容易に取得されるものでもないこと
- (ii) 業として使用されるときは、それを所有又は使用しない者よりもその所有者に対して有利性を与えることができること

³ TRIPs 協定の第7節に「開示されていない情報の保護」について規定があり、第39条第2項において、開示されていない情報について定義（要件として「秘密であること」、「（秘密であることにより）商業的価値があること」、「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」）があげられている。）が設けられている。

⁴ 法律 36/2009/QH12 号による改正後の法律 50/2005/QH11 号。条文の和訳は、<https://www.jetro.go.jp/ext_images/world/asia/vn/business/pdf/VN_20090619.pdf>参照のこと。本マニュアルにおいて、知的財産法の具体的内容に言及する場合は、上記 JETRO 仮訳を参照している（一部変更している場合もあり）。あくまで参考仮訳であるので、原文もご確認されたい。[最終アクセス日：2020年11月18日]

- (iii) それが開示されず、また容易に入手することもできないよう必要な措置を講じてその所有者が秘密を保持していること

日本とベトナムにおける営業秘密の法律上の定義を整理すると、営業秘密として保護され得る情報の種類が、日本においては、「技術上又は営業上の情報」の2つであるのに対し、ベトナムにおいては、「事業において利用可能な情報」と、より包括的に規定されている点が異なっている⁵。もっとも、かかる情報に要求される3つの要件、すなわち、(i)非公知性、(ii)価値性/有用性、(iii)秘密管理性は、類似していることが分かる。

なお、ベトナムにおいても日本同様、営業秘密の登録制度はない。

		ベトナム	日 本
根拠法令		知的財産法 (第4条第23項、第84条)	不正競争防止法 (第2条第6項)
構成要件	非公知性	公知でなくまた容易に取得されるものでもないこと	公然と知られていないこと
	価値性/有用性	所有又は使用しない者よりもその所有者に対して有利性を与えることができること	事業活動に有用であること
	秘密管理性	必要な措置を講じてその所有者が秘密を保持していること	秘密として管理されていること
情報の種類		事業において利用可能な情報	技術上又は営業上の情報

また、この定義からも明らかなとおり、ベトナムにおいても、営業秘密として法律上の保護を受けるためには、営業秘密の保有者が秘密保護措置を講じたことが必要である。つまり、秘密保護措置を講じない限り、企業にとっていかに重要な情報であったとしても、営業秘密とは認められず、法律上の保護を受けられない可能性が高い。

(2) 営業秘密の例外

以下の秘密情報は、営業秘密としては保護されないと定められている（知的

⁵ もっとも、企業において保護すべき営業秘密の多くは、製造技術、設計図面等の技術情報か、顧客リスト、経営戦略情報等の営業情報のいずれかに分類されることが一般的には多いと思われ、実質的には、日本・ベトナムの間に大きな相違はないように思われる。

財産法第 85 条)。

- (i) 身元に関する秘密⁶
- (ii) 国家管理の秘密
- (iii) 安全保障及び国防の秘密
- (iv) 事業に無関係な他の秘密保持情報

2. ベトナムにおける営業秘密所有者の権利

(1) 営業秘密所有者

ベトナム知的財産法において、「営業秘密所有者」とは、「適法に営業秘密を取得し、かつ、それを秘密に保持する組織又は個人とする。担当職務の履行中に担当職務を遂行する従業者又は当事者により取得された営業秘密は、全当事者による別段の合意がない限り、使用者又は職務割当者に属する。」と定義される（知的財産法第 121 条第 3 項）。

この規定からすれば、従業員が職務の過程で取得した営業秘密は、その使用者である会社に属すると解される。もっとも、情報の帰属について将来の疑義・紛争を避けるために、従業員との秘密保持契約等において、職務の過程で得られた秘密情報やそれを利用した知的財産等に関する権利が会社に帰属することを予め明確に合意しておくことが望ましいと考える。

(2) 営業秘密所有者の権利

ベトナム知的財産法において、以下の行為を営業秘密の使用として定義している（第 124 条第 4 項）。

- (i) 営業秘密を、製品の製造、サービスの提供又は商品の取引に適用すること
- (ii) 営業秘密を適用することにより得られた製品を販売し、販売のために広告し、販売用に保管し、また輸入すること

そして、営業秘密所有者は、第三者が無断で営業秘密を使用、開示等すること

⁶ ベトナムにおいても、個人のプライバシーに関する権利は保護されている（憲法第 21 条、民法第 38 条）。したがって、「身元に関する秘密」（参考英訳は **personal identification secret**）が営業秘密の保護対象から除外されている趣旨は、営業秘密に係る情報が個人情報としてプライバシー権の対象にもなる場合は、当該プライバシー権が優先するという点にあると考えられる。

を阻止する権利を有するとされるが、以下の行為についてはこれを阻止することはできないとされる（第 125 条第 3 項）。

- (i) 自らが非合法的に取得したことを知らずに又は知る義務を有せずに取得した営業秘密を開示し又は使用すること。
- (ii) 第 128 条第 1 項⁷の規定に従い公衆を保護するために営業秘密を開示すること。
- (iii) 非商業目的で第 128 条に従い秘密資料を使用すること。
- (iv) 他人が独立して創出した営業秘密を開示し又は使用すること。
- (v) 適法に頒布された製品の分析又は評価の結果生じた営業秘密を開示し又は使用すること。ただし、分析者又は評価者と営業秘密の所有者又は当該製品の供給者との間に別段の合意がある場合は、この限りでない。

3. ベトナムにおける営業秘密侵害行為の定義

(1) 知的財産法上の定義

知的財産法上、次の行為は営業秘密侵害行為とみなされる（第 127 条）。

- (i) 営業秘密の適法管理者（当該営業秘密所有者、その者の適法な実施権者又は管理職を含む。）により取られた秘密保持措置に反する行為をなすことにより、営業秘密の具体的情報を入手又は取得すること。
- (ii) 営業秘密所有者の許可なしに営業秘密の具体的情報を開示又は使用すること。
- (iii) 秘密保持契約に違反すること又は営業秘密を入手、取得若しくは開示するために秘密保持担当者を欺瞞し、誘導し、買収し、強要し、唆し若しくはその信用を濫用すること。
- (iv) 営業秘密の具体的情報であって、製品に関する営業又はマーケティングのラ

⁷ 知的財産法第 128 条では、「法律により、医薬品又は農業用化学製品に関して営業又はマーケティングのライセンスを申請する申請人が、試験資料又は営業秘密である何らか他の資料であって、その作成に相当の努力又は経費を伴うものの提出を要求する場合、かつ、申請人が当該資料の秘密保持を請求する場合は、当該資料について、当局は、開示することが公衆を保護するために必要な場合を除き、それが不公正な商業目的に使用されることも、又は開示されることもないように必要な措置を取る義務を有する」と、試験資料の秘密保持義務を定めている。

イセンス付与のための手続に基づいて他人により提出されるもの⁸を、所管当局により取られた秘密保持措置に反する行動により、入手又は取得すること。

- (v) 営業秘密を、それが上記(i)、(ii)、(iii)及び(iv)にいう行為の1に従事する他人により取得されたことを知りながら又は知る義務を有しながら、使用し又は開示すること。
- (vi) 知的財産法第128条に規定する秘密保持義務を履行しないこと。

⁸ ベトナムにおいては、マーケティングを行ったり特定の製品を販売したりするうえで、所定の法令によりライセンスを取得する必要がある場合がある。このような場合には、申請者にて、当該マーケティング事業や製品について詳細を説明する資料を当局に提出することが多いが、その資料に営業秘密が含まれている可能性がある。

日本の不正競争防止法で列挙される営業秘密侵害行為（第 2 条第 1 項第 4 号から第 10 号、第 21 条）と比較した場合、下表のとおりとなると考えられる。

	ベトナム	日 本
根拠法令	知的財産法（第 127 条）	不正競争防止法（第 21 条第 1 項/ ベトナム法に対応する要旨のみ抜粋）
不正取得類型	・営業秘密の適法管理者（当該営業秘密所有者、その者の適法な実施権者又は管理職を含む）により取られた秘密保持措置に反する行為をなすことにより、営業秘密の具体的情報を入手又は取得すること（第 a 号）。 ・営業秘密の具体的情報であって、製品に関する営業又はマーケティングのライセンス付与のための手続に基づいて他人により提出されるものを、所管当局により取られた秘密保持措置に反する行動により、入手又は取得すること（第 d 号）。	・図利加害目的で、詐欺等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（第 1 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（第 2 号）

正当取得類型	・営業秘密所有者の許可なしに営業秘密の具体的情報を開示又は使用すること（第 b 号）。 ・知的財産法第 128 条に規定する秘密保持義務を履行しないこと（第 c 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）媒体等の横領、（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（第 3 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（第 4 号） ・営業秘密を保有者から示された現職の役員又は従業者が、図利加害目的で、その営業秘密の管理に係る任務に背き、営業秘密を使用又は開示する行為（第 5 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（第 6 号）
転得類型	・営業秘密を、それが上記第 a 号、第 b 号、第 c 号及び第 d 号に定めるいずれかの行為に従事する他人により取得されたことを知りながら又は知るべきながら、使用し又は開示すること（第 d 号）。	・図利加害目的で、第 2 号、第 4 号～第 6 号の罪に当たる開示（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（第 7 号） ・図利加害目的で、第 2 号、第 4 号～第 7 号の罪に当たる開示（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 次以降の転得者をすべて対象) (第 8 号)
侵害品譲渡類型		・ 図利加害目的で、第 2 号、第 4 号～第 8 号の罪に当たる使用 (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 (第 9 号)
教唆・幫助	・ 秘密保持契約に違反すること又は営業秘密を入手、取得若しくは開示するために秘密保持担当者を欺瞞し、誘導し、買収し、強要し、唆し若しくはその信用を濫用すること (第 c 号)	(民法第 719 条、刑法第 61 条、第 62 条)

(2) 競争法、サイバーセキュリティ法における営業秘密侵害行為

知的財産法における営業秘密侵害行為の定義は上記 3.(1)のとおりであるが、秘密情報の漏えいについては、以下のとおり、競争法⁹及びサイバーセキュリティ法¹⁰にも関連する規定がある。

① 競争法

営業上の秘密情報について、以下の態様により侵害することは、不公正な競争行為として禁止される (第 45 条第 1 号)。

- (i) 営業上の秘密情報について、所有者が講じるセキュリティ保護措置に反して、当該秘密情報にアクセスすること、又は同情報を取得すること。
- (ii) 営業上の秘密情報について、所有者の許可なく、開示又は使用すること。

競争法では、上記のとおり、「営業上の秘密情報」という用語を使用しており、

⁹ 法律 23/2018/QH14 号

¹⁰ 法律 24/2018/QH14 号

知的財産法で定義・保護される「営業秘密」とは別の概念と解される。そして、競争法の「営業上の秘密情報」には、「営業秘密」として保護されるための 3 要件は必要なく、「営業秘密」として法令上の保護を受けるものよりも広い範囲の秘密情報が含まれると解される。これは、競争法の目的が公正な競争の確保にあることから、より広い範囲の秘密情報漏えい行為を禁止することを意図したものと考えられる。

一方で、競争法における秘密情報の侵害行為は 2 つの行為のみが挙げられており、知的財産法で規定される営業秘密侵害行為よりも行為の範囲は狭い¹¹。

② サイバーセキュリティ法

インターネット等のオンラインサービスを通じた脅威から国家的・社会的利益を保護することを目的として、サイバーセキュリティ法が 2018 年 6 月 12 日に成立し、2019 年 1 月 1 日に施行されている。

同法において、以下の行為は、サイバー空間における諜報活動又は秘密情報の漏えい行為として禁止されると定められている（第 17 条）¹²。

- (i) 国家機密、職務上の秘密、業務上の秘密、営業上の秘密、家族に関する秘密、プライバシーに分類される情報を不正に入手、取引、収集、故意に漏えいし、他の組織又は個人の尊厳、名誉、適法な権利/利益を侵害する行為。
- (ii) サイバースペース上で送信又は保存される国家機密情報、業務上の秘密、営業上の秘密、家族に関する秘密、プライバシーに分類される情報を故意に削除したり、損害を与えたり、紛失したり、変更したりすること。
- (iii) 国家機密情報、業務上の秘密、営業上の秘密、家族に関する秘密、プライバシーに分類される情報を保護するための技術的措置を故意に変更、中止、又は無効化すること。
- (iv) 国家機密情報、業務上の秘密、営業上の秘密、家族に関する秘密、プライバシーに分類される情報を法律に反してサイバースペースに掲示すること。
- (v) 不法に会話を盗聴又は録音すること。
- (vi) その他、国家機密情報、業務上の秘密、営業上の秘密、家族に関する秘密、プライバシーに分類される情報をサイバースペース上で故意に侵害していると認められる行為。

¹¹ ベトナム司法省ホームページ参照。 <https://moj.gov.vn/qt/tintuc/Pages/nghien-cuu-trao-doi.aspx?ItemID=2537> [最終アクセス日：2020 年 11 月 18 日]

¹² 通信サービスプロバイダー等に対する処罰規定はあるが（政令 15/2020/ND-CP 号第 79 条、第 80 条、第 100 条等）、その他の違反者に対する罰則はまだ制定されていない。

4. ベトナムにおける営業秘密侵害の実態

(1) ベトナムにおける営業秘密侵害の3つのパターン

上述のとおり、法律上の営業秘密侵害行為の定義は、日本法とベトナム法とで具体的な規定内容は異なっているものの、営業秘密・秘密情報の漏えい・流出が実際に発生するルートに着目した場合、そのパターンは、①従業員漏えい型、②取引先漏えい型、③第三者不正取得型の3つに分類されることは、日本もベトナムも大きく変わることはない。

そこで、以下では、この3つのパターン別に、ベトナムにおける営業秘密侵害の実態について説明する。

(2) 従業員漏えい型

これは、企業が雇用した従業員が、在職中又は退職後に、企業の営業秘密・秘密情報を漏えいするというパターンである。なお、正規雇用に限らず、派遣従業員などによる営業秘密漏えいも含まれる。紹介する3パターンの中では、ベトナムにおいてはこの従業員漏えい型が最も多くを占めていると思われる。

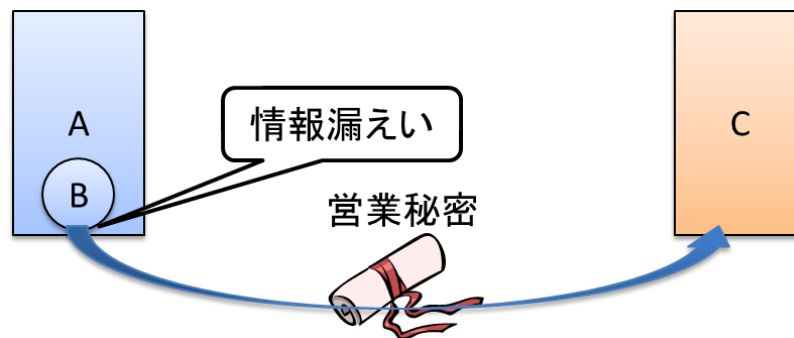
従業員漏えい型は、さらに、次の3つのパターンに分類することができる。

- ① 従業員が在職中に、競合企業等に営業秘密を漏えい
- ② 従業員が退職後、転職先の企業に営業秘密を漏えい
- ③ 従業員が自ら競合会社を設立して、営業秘密を流用

以下、順にみていく。

① 従業員が在職中に競合企業等に営業秘密を漏えい

これは、自社（下図 A 社）の従業員 B が、在職中に、自社の競合企業 C 社に対して、営業秘密の漏えいを行うというパターンである。



例えば、物流を行う日系企業（上図で A に該当）では、従業員（上図で B に該当）が、在職中に、同社の内部文書（契約書のひな型や顧客に関する情報）を競合企業（上図で C に該当）に漏えいし、その後 B が A を退職して C の役員に就任したという事件が発生している。

② 従業員が退職後、転職先の企業に営業秘密を漏えい

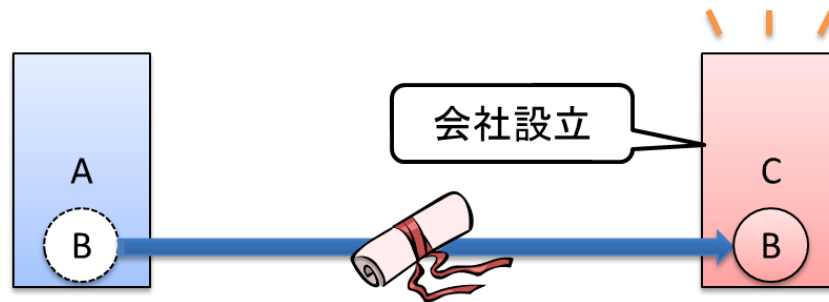
これは、自社（A 社）の従業員 B が、A 社を退職して競合企業 C 社に転職し、C 社にて前勤務先の A 社の営業秘密を利用したり、開示したりするパターンである。



例えば、自社機器の販売を行う日系企業（上図で A に該当）では、従業員（上図で B に該当）が、退職して競合企業（上図で C に該当）に就職し、A の就業規則にあった退職後の秘密保持義務に違反して、A に在職中に受けていた A 製品のクレーム情報等の秘密情報を利用して C で営業活動を行うという事件が発生している。

③ 従業員が自ら競合会社を設立して、営業秘密を流用

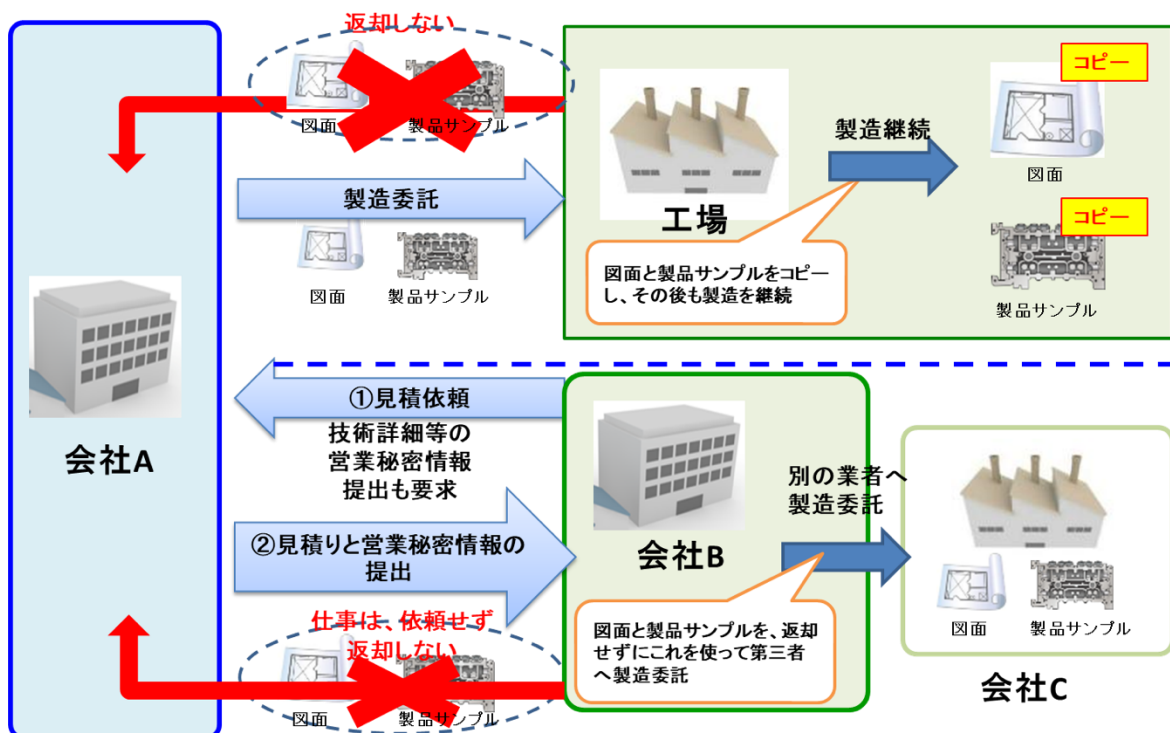
これは、自社（A 社）の従業員 B が、A 社を退職して、あるいは、在職中に、A 社と競合する C 社を設立し、そこで A 社の営業秘密を流用するというパターンである。



例えば、ベトナムで消費者向け製品の製造を行う日系企業（上図で A に該当）では、従業員（上図で B に該当）が、在職中に自らの会社（上図で C に該当）を立ち上げ、A の設計図面等の営業秘密を利用して、A の製品と類似の製品の製造販売を行っていたという事件が発生している。

(3) 取引先漏えい型

このパターンは、下請け・製造委託先又は顧客といった、取引先から営業秘密が漏えい・流出する、又は不正使用されるというパターンである。



(図 1)

① 下請けから営業秘密が漏えいするパターン（図 1 上段参照）

このパターンには、例えば、ベトナム企業に金型等の製造を委託する場合に、当該委託先が、提供を受けた図面や製品サンプルを、委託関係終了後も返還をせずに、無断で使用して同一物品を製造し、競合他社に販売するといったケースが該当する。

② 顧客から営業秘密が漏えいするパターン（図 1 下段参照）

このパターンには、例えば、顧客であるベトナム企業 B からの見積依頼の際に、B 社の要求に応じて図面や製品サンプルなどの営業秘密情報を提供したところ、B 社がそれらを別のベトナム企業 C 社に交付し、C 社に同じ製品をより安価に製造させるといったケースが該当する。

このパターンについて、営業秘密侵害責任を追及しようとする、C 社が B 社を通じて A 社の営業秘密を取得したことを証明することが必要となるが、その立証は一般的には難しいと考えられる。しかし、このような場合でも、同じ図面やサンプルに基づき製造された製品は、製品の構造や機能などが必然的に似てくると考えられるため、そうした構造や機能についての特許権などを別途確保し、登録権利に基づき、C 社に対して権利行使を行うことを検討すべきである。

このように、1つの製品について、営業秘密として保護すべき部分と、特許権などの登録権利によって保護すべき部分を的確に峻別し、1つの製品について多角的に知的財産権を組み合わせることによって保護するという視点が、非常に重要となってくる。

なお、ベトナムにおける特許出願の留意点については後述第 2 章 3.(3)を参照されたい。

(4) 第三者不正取得型

このパターンは、日本の不正競争防止法における営業秘密侵害行為に関する法律上の定義のうち、「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」（第 2 条第 1 項第 4 号）に該当するものであり、例えば、ハッキングなどの行為によって営業秘密が盗用された場合などが該当する。

(5) 新たな侵害形態

① インターネット上での漏えい

以上は、漏えいの「ルート別」に営業秘密侵害を類型化したものであるが、漏えいの「手段」に着目したとき、インターネット上での新たな侵害形態が散見されるのも、ベトナムにおける営業秘密侵害の特徴の1つとなっている。

例えば、建設物の設計図面を映像化する業務をベトナム企業に委託していたところ、当該ベトナム企業では作成した映像を保存するのに、クラウドストレージの代わりとして **Youtube** を利用しており、その公開設定を誤って映像が誰でも閲覧可能な状態にあったという事件が発生している。インターネット上でのデータ保存等が一般化している一方で、当該保存を行う者の情報セキュリティに関する認識が甘い等の理由により意図しない情報の流出事例は少なくなく、今後も増加することが予想される。

② テレワーク時における秘密情報の漏えい

昨今の情勢に鑑み、ベトナムにおいてもテレワークを導入する企業が多く見られる¹³。テレワーク環境を整える上では、紙資料等の社外への持ち出しの取り扱い、携帯電話や私用 PC といった社外端末から社内データへのアクセス、オンライン会議での画面共有時の情報漏えい、チャットツール等 SNS の使用頻度の高まり等、営業秘密を保護する上で対応を検討すべき新たな課題が発生している。

これらの課題への対応については、日本の考え方と共通することも多いので、経済産業省の「テレワーク時における秘密情報管理のポイント（Q&A 解説）」を参考としつつ¹⁴、社内ルールを明確にすることが望ましいといえる。

5. 営業秘密侵害に対する法的措置

ベトナムにおいては、営業秘密侵害行為に対しては、民事的救済及び行政措置の2つの手段を取り得る。営業秘密侵害行為に対する制裁が、行政措置の対象となって刑事制裁の対象とならない点は、日本とは異なる¹⁵。もともと、2018年

¹³ コロナウィルス対策の一環として、企業に対して従業員の在宅勤務を強化するよう求める首相指示や各地方自治体による通知が複数発出され、これに応じる形でテレワークを導入する企業が増加した。

¹⁴ https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/teleworkqa_20200507.pdf [最終アクセス日：2020年11月18日]

¹⁵ 2009年に改正される前の旧刑法では、産業財産権を侵害する罪として一般的に規定されていたため（第171条）、営業秘密侵害も刑事罰の対象となり得ると考えられていた。しかしながら、2009年の刑法改正では、産業財産権侵害罪の対象となるのは商標権と地理的

12月30日に発効したCPTPP（環太平洋パートナーシップに関する包括的及び先進的な協定（TPP11協定））への加盟にあたって、ベトナムには、営業秘密侵害の刑事罰化について3年の経過措置が設けられており、今後刑事罰導入の議論がどのように進展するのか動向が注目される。

なお、民事的救済及び行政措置のいずれについても、公式の統計情報は公開されていないため、その実情は不明である。ベトナムにおいて、営業秘密保護の意識が定着していないこともあり、営業秘密侵害行為に関する民事裁判や行政措置が利用されることはまだ限定的であるように思われる。

	ベトナム	日本
民事的救済 (知的財産法第202条)	裁判所は、知的財産権の侵害行為を犯した組織及び個人に対処するため、次の民事救済措置を講じる。 ・知的財産権の侵害の終了を強制すること ・評判の是正及び謝罪を強制すること ・民事的義務の遂行を強制すること ・損害に対する補償を強制すること ・知的財産権侵害商品の創出又は取引に主として使用された商品、素材及び用具について、廃棄、非商業目的での頒布又は使用を強制すること。ただし、当該頒布及び使用が知的財産権所有者による権利行使に影響を与えないことを条件とする。	・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
行政措置 (知的財産法第214条)	・行政機関（市場監督管理局）による摘発 ・行政措置の内容は、主たる行政罰（警告、過料）、追加的行政罰（知的財産権の偽造商品及び当該偽造商品の製造又は取引に主として使用された素材・原材料及び用	・なし

表示が侵害された場合であると明確に規定されたため、現行刑法の下では、営業秘密侵害は刑事罰の対象とならないと解される。

	具の没収、関係事業活動の一定期間の停止)、及び是正措置(知的財産権侵害品の強制破壊、ベトナムの領土からの強制撤去等)	
刑事制裁	・なし	・捜査後、起訴されれば刑事訴訟 ・刑事罰の内容 (国内での侵害の場合) 個人については、10年以下の懲役、2000万円以下の罰金又はこれらの併科。法人については、5億円以下の罰金。 (国外での侵害の場合) ①日本国外における使用目的で営業秘密を不正に取得・領得した者、②相手方が日本国外における使用目的を有することを知りながら営業秘密を不正に開示した者、及び③日本国内の事業者が保有する営業秘密を日本国外において不正使用した者について、個人については、10年以下の懲役、3000万円以下の罰金又はこれらの併科。法人については、10億円以下の罰金。

以下、それぞれについて概説する。

(1) 民事的救済

① ベトナムの民事裁判制度

まずは、民事的救済について概説する前提として、ベトナムの民事裁判制度について簡単に述べる。ベトナムの裁判所は二審制を採用している（民事訴訟法¹⁶第17条第1項）。第一審は、原則、職業裁判官1名と一般市民から選ばれた参審員2名から構成される（民事訴訟法第63条）。第二審は、職業裁判官3名で

¹⁶ 法 92/2015/QH13 号

構成される（民事訴訟法第64条）。

なお、確定判決において法令適用に重大な誤りがある場合に、その誤りを是正する監督審がある。また、判決確定後に新しく重要な事実関係が発見された場合に、事実認定を是正する再審の制度もある。もともと、監督審と再審は、原則として、最高人民裁判所長官又は最高人民検察院長官にのみ申立権が認められており、当事者は申立てできない。その意味でも、監督審・再審は、三審制とは異なる。

また、裁判は原則公開であるが、営業秘密が開示されるおそれがある場合等に非公開となることもある（民事訴訟法第15条第2項）。

ベトナムの民事裁判では、和解前置主義が取られており、審理前に裁判所主導による和解調停手続が設定される（民事訴訟法第180条）。ここで和解が成立しない場合に、審理へ移行する。

現在、ベトナムには知的財産権を審理する専門の裁判所はない¹⁷。

② 営業秘密侵害行為に対する民事的救済

ベトナムの知的財産法では、営業秘密侵害者に対する民事訴訟により、裁判所が、侵害行為の差止め、損害賠償、評判の是正及び謝罪、民事的義務の遂行等の救済手段を講じることができるとしている（知的財産法第202条）。損害賠償を請求する場合、その額は、以下の(i)～(iii)を基準に、その順序に従って算定されることになる（知的財産法第205条第1項）。また、ベトナムでは、いわゆる「懲罰的損害賠償制度」は認められていない。

- (i) 原告の利益減少分が全物理的損害に含まれていないときは、金額により決定された全物理的損害に侵害の結果として被告が得た利益を加算した額
- (ii) 知的財産権対象の使用に係る合意に基づいて、犯された侵害行為と同等程度まで知的財産権対象を使用する権利を被告が原告から移転されたと想定して、当該知的財産権対象を使用する権利の移転の価値
- (iii)(i)と(ii)に従い補償金額を決定することが不可能な場合は、当該金額は、損失レベルに応じて裁判所により決定されるが、500,000,000 ベトナムドン（250万円相当）を超えないものとする。

なお、ベトナムにおいては、実際に営業秘密侵害行為に基づいて損害賠償が認

¹⁷ 省級裁判所では「裁判官委員会、刑事法廷、民事法廷、経済法廷、労働法廷、行政法廷」の分類があり（民事訴訟法第27条第1項）、営業秘密を含む知的財産権関連事件は主として民事法廷又は経済法廷で扱われている。一方、県級裁判所についてはそのような組織分けはなされていない。

められた裁判例は公表されているデータベースの検索では確認できず、実際どのように損害額が認定されるかは予測できないところがある。

(2) 行政措置

行政措置とは、日本にはない法的措置であり、具体的には、行政機関により侵害品の没収、営業停止命令、過料等の措置が命じられる。

管轄行政機関は、侵害行為の性質又は程度に応じて、以下の罰則を科すことができる（政令 99/2013/NĐ-CP 号第 3 条）。

- ・ 警告
- ・ 過料
- ・ 侵害品の没収又は破壊
- ・ 営業の一時停止
- ・ 改善措置

知的財産権侵害行為に関する行政措置の所管官庁は、科学技術検査官（Thanh tra Khoa học và Công nghệ）、市場管理局（Quản lý thị trường）、税関（商品の再輸出、輸入の場合）がある（政令 99/2013/NĐ-CP 号第 15 条第 1 項、第 3 項、第 4 項）。その役割分担としては、特許権等の専門的知識を有する摘発については科学技術検査官、市場での模倣品の摘発等一般的な知的財産権侵害については市場管理局、水際での侵害品差止については税関が担当するとされている。

なお、行政措置後に、侵害者に対して民事訴訟を提起して、差止請求又は損害賠償請求することも可能である（政令 105/2006/NĐ-CP 号第 4 条第 1 項）。

6. 営業秘密に関する法規制の改正状況

かつて営業秘密の定義・保護要件は、政令、競争法で規定されていたが、2005 年に知的財産法が制定されると、同法にて定義・保護要件が規定されることになり、今に至っている。下表のとおり、その内容について大きな変更点はない。

法令	定義・保護要件	備考
政令第 54/2000/NĐ- CP 号	(第 6 条第 1 項) 保護される営業秘密とは、次のすべての条件を満たした情報の形式の成果である。	

(失効)	(1) 公知でないこと (2) 業として使用されるときは、それを所有又は使用しない者よりもその所有者に対して有利性を与えることができること (3) それが開示されず、また容易に入手することもできないよう必要な措置を講じてその所有者が秘密を保持していること	
2004 年競争法 (失効)	(第 3 条第 10 項) 営業秘密とは、次のすべての条件を満たした情報をいう。 (1) 公知でないこと (2) 業として使用されるときは、それを所有又は使用しない者よりもその所有者に対して有利性を与えることができること (3) それが開示されず、また容易に入手することもできないよう必要な措置を講じてその所有者が秘密を保持していること	上 記 政 令 第 54/2000/ND-CP 号に定めた営業秘密の保護条件と同じ。
2005 年知的財産法 (2009 年知的財産法により一部改正)	(第 4 条第 23 項) 営業秘密とは、財政的投資、知的投資から得られた情報であって、開示されておらず、かつ、営業において利用可能な情報である。 (第 84 条) 営業秘密は、次の要件を満たした場合、保護に適格とする。 (1) 公知でなく、<u>また容易に取得されるものでもないこと</u> (2) 業として使用されるときは、それを所有又は使用しない者よりもその所有者に対して有利性を与えることができること (3) それが開示されず、また容易に入手することもできないよう必要な措置を講じてその所有者が秘密を保持していること	上記 2004 年競争法の営業秘密の定義とほぼ同じだが、((1)で「容易に取得されるものでもない」という要件が追加された。
2009 年知的財産法 (2019 年に)	(第 4 条第 23 項) 2005 年知的財産法から変更なし	

一部改正) (有効)	(第 84 条) 2005 年知的財産法から変更なし	
---------------	-------------------------------	--

営業秘密侵害行為に対する制裁の改正状況は、以下のとおりである。

法令	内容	改正のポイント
政令 120/2005/ND-CP 号 (失効)	【過料】 営業秘密の不正収集・不正開示・不正使用、又は営業秘密の不正収集・不正開示・不正使用を目的として秘密保持契約等の違反行為を行った者は、5,000,000～10,000,000 ベトナムドン（2 万 5 千～5 万円相当）が科される。当該秘密情報を使用し、2 省以上の範囲で商品を製造し、提供する場合は、又は当該秘密情報をその所有者の競業他社に提供する場合、上記の 2 倍の金額が科される（第 31 条第 1 項）。 【追加制裁】 違反行為から得た利益の没収を含む、違反行為に用いた道具・物的証拠の没収（第 31 条第 3 項）	
政令 97/2010/ND-CP 号（失効）	【過料】 営業秘密権の侵害行為を行った者は、10,000,000～30,000,000 ベトナムドン（5 万～15 万円相当）が科される（第 14 条第 9 項） 【追加制裁】 ・違反行為の手段・物的証拠の没収 ・違反した商品の取引の 6 か月までの活動の停止（第 14 条第 11 項） 【克服措置】 ・侵害要素の強制的な除去、侵害要素の強制的な除去ができない侵害商品の強制破壊 ・侵害行為から得た利益の没収	過料金額が増加し、追加制裁・克服措置も厳格化

	(第 14 条第 12 項)	
政令 99/2013/NĐ- CP 号 (有 効)	【過料】 営業秘密権の侵害行為を行った者は、個人の場合は 5,000,000～15,000,000 ベトナムドン (2 万 5 千円～7 万 5 千円相当)、組織の場合にはその 2 倍の過料が科される (第 14 条第 15 項、第 2 条第 2 項) 【追加制裁】 侵害商品・サービスに関する取引の 1 か月～3 か月の活動の停止 (第 14 条第 17 項) 【克服措置】 ・侵害要素の強制的な除去、侵害要素の強制的な除去ができない侵害商品の強制破壊 ・侵害行為から得た利益の没収 (第 14 条第 18 項)	過料金額について個人と組織を区別させるも、組織の過料額は従前と変更無し。追加制裁の営業停止期間が短縮された。
政令 75/2019/NĐ- CP 号 (有効)	【過料】 競争法で定める「営業上の秘密情報」に対する不正アクセス・不正収集・不正開示・不正使用を行った者は、個人の場合には 200,000,000 ～ 300,000,000 ベトナムドン (100 万～150 万円相当)、組織の場合にはその 2 倍の過料が科される。 (第 16 条 1 項、第 4 条第 7 項) 【追加制裁】 ・違反行為に用いた道具・物的証拠の没収 ・違反行為から得た利益の没収 (第 16 条 2 項)	知的財産法上の営業秘密侵害行為に対する過料と比べると金額が大きい。

7. 営業秘密規定の域外適用

営業秘密規定の域外適用について、前述の通り、日本の不正競争防止法において国外犯処罰・海外重課の規定があるところ、その他については、法の適用に関する通則法の解釈によることが考えられる。詳細は経済産業省の「渉外事案の適用関係の概略と民事訴訟における考えられる主張ポイント集」を参照されたい

18。

一方、ベトナムにおいて、営業秘密侵害に関する域外適用の規定はない。もっとも、ベトナム国内での侵害に限定するという規定があるわけでもないので、理論上は域外適用の余地があると考えられる。なお、行政措置に関しては、域外適用される対象者はベトナム国外で違反行為を行ったベトナム人又はベトナムで設立された組織（ただし、日本企業のベトナム子会社もベトナム法人として扱われると考えられる。）に限定されると解される（行政違反処分法¹⁹第 20 条）。

8. 裁判例

社会主義国家であるベトナムでは、国会が国家の最高権力機関であり、憲法、法律及び国会常務委員会令の解释权は国会常務委員会の権限とされ、裁判所は法の適用を担うとされていた。しかしながら、この状況では、ベトナム国内裁判において過去の裁判例が先例として参照されないために、裁判所の判断が安定せず予測可能性が低いことが課題と考えられていた。

そこで、選定された一部の裁判例に先例拘束力を与え、法源の一つとする判例制度が 2016 年に導入された。ただし、判例として選定される裁判例は毎年 8 件程度で、2020 年 11 月時点で 39 件に過ぎず、加えて、営業秘密侵害に関連した事件で判例として選定されたものは現時点では存在しない。また、判例以外の裁判例についても、2016 年以降の全判決が裁判所のウェブサイトで公開されているが、営業秘密侵害が訴訟に発展するケースは珍しく、営業秘密侵害に関連した事件で裁判例が公開されている事件も確認できず、競業避止義務が問題となった裁判例が数件確認できる程度である²⁰。また、競争法違反事例においても、秘密情報の侵害が問題となった事例も公表されていない。

¹⁸ https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/202006_pointcollection.pdf [最終アクセス日：2020 年 11 月 18 日]

¹⁹ 法律 15/2012./QH13 号

²⁰ ベトナム最高人民裁判所ウェブサイト（<https://congbobanan.toaan.gov.vn/>）参照。[最終アクセス日：2020 年 11 月 18 日]

第2章 一営業秘密漏えい対策実践編一

1. 総論

(1) 管理体制の構築を考える上での2つの視点

営業秘密を含めて企業が保有する重要情報の意図しない漏えい・流出を防ぐためには、どのような管理体制を構築していくべきか。そのゴール、すなわち、あるべき管理体制の全体像がイメージできなければ、具体的にやるべきことは見えにくいであろう。

情報への管理体制を整備する本来の目的は、営業秘密などの情報の漏えいをできる限り防止・抑止することである。一方、もし情報漏えいが発生した場合に、民事訴訟や行政措置を通じた営業秘密侵害に対する法的救済を求めるためには、侵害された情報が、法律上の営業秘密に該当していなければならないところ、上述のように、そのための要件として、営業秘密保有者が当該秘密情報に対して、「秘密保護の措置」を取っていたこと（秘密管理性）が必要である。

しかしながら、ベトナム法においては、具体的にどのような措置を講ずれば、法律上、「秘密保護の措置」をとったと認められるかについて定めた指針やガイドラインは確認できない。実効的に漏えいを防止・抑止する物理的・人的管理体制を整備し、これを運用していくことが、情報の漏えい防止、ひいては法律上の秘密管理性要件を満たすことにつながると考えられるので、以下そのような体制の整備について検討すべき点を述べる。

(2) 漏えい対策実効性の観点からの管理体制の構築

営業秘密の漏えいを実効的に防止するためには、物理的管理体制、人的管理体制の両側面から対策を強化する必要がある。それぞれのポイントは、以下のとおりである。

① 物理的な管理体制の整備

上述のとおり、ベトナムにおいては営業秘密の漏えい防止を強化するための物理的管理体制について具体的な指針等は公表されていない。しかしながら、営業秘密が保護される要件は日本と同様であることから、基本的には日本で行うべき管理体制の整備と共通する点は多いと考える。なお、日本における営業秘密を含む企業が保有する重要情報の物理的な管理体制の整備については、ハンド

ブックに詳しく説明されており、ベトナムにおける物理的な管理体制の整備・構築するに際しても、大変参考になるので、是非参照されたい。

その上で、ベトナムにおける物理的な管理体制の整備を考えるにあたっては、特に以下の事項を考慮する必要がある。

- ・ 労働者の流動性が高いベトナムでは、上述のように、(元)従業員による営業秘密侵害の被害が従来から多く発生しており、もともと地域的リスクが高いことに加えて、日系企業の営業秘密は、その価値の高さゆえに、狙われやすい。日本と同等、あるいは、それ以上に、管理体制を整備する必要がある。
- ・ ベトナムでは、携帯電話及び SNS が業務上でも利用されることが珍しくなく、営業秘密漏えい防止の観点からは、これらへの対策が必須である(→4.(2)④参照)。
- ・ 物理的な管理体制の強化としては、静脈認証等の技術的により高度なアクセス制限手法を導入することが考えられるが、ベトナムにおいては高度な技術を導入することについてコストや取扱業者がいない等の理由により事実上不可能な場合もある。このため、日本の管理体制水準に合わせることは現実的には難しい場合もあるということに留意した上で、代替できる手段や次善の手段がないかについて検討する等、現場の状況にあわせて柔軟に対応していく必要がある。

② 人的管理体制の整備

人的管理体制は、「対社内」つまり、自社の従業員の管理と、「対社外」つまり、自社の取引先の管理の両面から整備する必要があるが、いずれについても、秘密保持契約をはじめとする契約、規程類の整備がその柱となる。規定すべき具体的な事項については、ここでも「対社内」、「対社外」のそれぞれ、日本と共通する部分も多いが、労働法等のベトナムの関係法令等の適用に注意する必要がある。

人的管理体制の整備において、ベトナムで特に注意すべき事項は、以下のとおりである。

- ・ 日本人とベトナム人との考え方は、異なるところが多い。営業秘密の重要性について理解しているベトナム人も近年増えてきてはいるが、工員などのような一般職員まで含めた場合、全体的には、営業秘密保護意識は不十分であると言わざるを得ない。研修を含めた啓発活動が重要である(→4.(2)⑥参照)。
- ・ 特に、競業制限については、労働者の権利・職業選択の自由を侵害していると判断されないよう十分な配慮をすることが必要である(→4.(2)③参照)
- ・ 日系企業の場合、秘密保持義務や競業避止義務については、一旦、契約を締

結しただけで対応を終わらせがちであるが、締結した契約上の義務がそのとおりに履行されているとは限らない。また、仮に契約違反が発覚したとしても、判例制度も未熟であるベトナムにおいて権利の執行をすることは現実的ではない。取引関係に入る前に、本当に契約内容を守れる相手であるのか、信用調査等を行うことも考えられる。法律的、形式的な対応にとどまらず、場合によっては、そうした現実的な対応も検討する必要があるだろう。

- ・ 日系企業の場合、顧客の言われるままに秘密情報を開示してしまったり、例えば身分証の提示を求めるといった、日本と異なる対応をためらいがちである。しかし、上述のとおり、地域的リスクが高いベトナムで、対応をより強化するのは自然なことであり、むしろ、顧客のベトナム企業の方が、そうした「性悪説」ベースの対応に慣れていることも少なくない。顧客に対して「日本式」の遠慮は危険であり、無用である。

2. 管理体制整備のステップ1ー管理体制の現状の確認

前節において、ベトナムにおける管理体制整備の基本的な視点について説明した。これを踏まえて、ここからは、具体的な管理体制の構築手法についてみていく。

(1) 現状把握の必要性

管理体制整備の第一歩は、まず、現状を把握することである。日系企業の場合、日本本社では、営業秘密管理についての社内規程や秘密保持契約のひな型等が存在するにもかかわらず、ベトナム拠点では、こうした規程類がうまく展開、活用されず、体制整備が手付かずの状態であることも、大企業も含めて少なくなく、しかも、そうした現状を誰も把握していない例も散見される。

まずは、営業秘密管理についての体制が具体的にどこまでなされていて、何が欠けているのか、現状を把握することが必要となろう。

(2) セルフチェックシート

現状把握のために便利なのが、支援事業で利用されている「セルフチェックシート」である。これは、上述 1.の総論で説明した視点に基づき、ハンドブックをベースにしつつ、ベトナム特有の注意点を加味して、管理体制についてチェックすべきポイントをまとめたものである。カテゴリ別に重要項目が列挙され、自社

の弱点を容易に把握できるので、ぜひ活用して頂きたい。

セルフチェックシート

カテゴリ	項目
秘密情報の特定	☐ 保有情報をリスト化している
	☐ 保有情報の区分をし、秘密情報を特定している
	☐ 秘密の重要度に応じたアクセス権者を決めている
管理方針の策定	☐ ベトナム法に基づいて作成された営業秘密管理規定や管理マニュアルを策定している
	☐ 各拠点に営業秘密管理責任者を置いている
物理的管理 (執務室)	☐ 秘密の記録媒体に「contorolled copy」等の秘密表示がされている
	☐ プリンターの利用者記録を確認することができる
	☐ 一般情報と分離して保管し、紙媒体等は鍵付きキャビネットに保管されている
	☐ 持ち出しの際の盗難防止策がとられている
	☐ 複製を制限するルールが定められている
物理的管理 (生産現場等)	☐ 外部の者が立ち入る際には、部外者と認識できるようバッジ等をつけている
	☐ 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
	☐ 工場内では携帯電話を使用できる職員が限られている、若しくは禁止されている
	☐ 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り方を制限している
	☐ 立ち入り制限エリアを適切に管理できている(警備員の配置、入退室記録等)

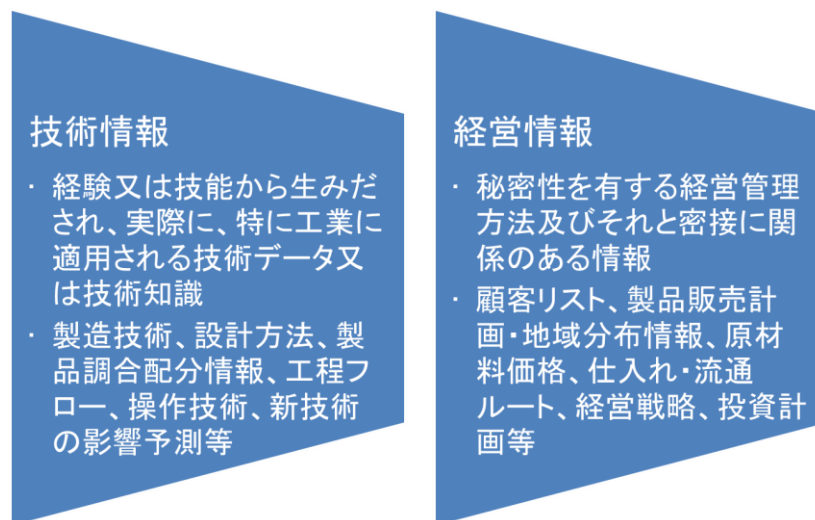
技術的管理	☐ 保有する電子データはサーバー上で管理している
	☐ 秘密情報を管理する PC に対して外部からの侵入に対する防護策をとっている
	☐ 従業員の PC にパスワードを設定している
	☐ チャットアプリの使用を禁止・制限している
	☐ 私物の USB メモリ等記録媒体の利用を禁止・制限している
	☐ 秘密の度合いに応じて管理者の特定、アクセス権者の限定をしている
	☐ 複製使用後、情報が読み取れないような廃棄方法が徹底されている
人的管理	☐ 定期的に研修を行い営業秘密保護の重要性を周知喚起している
	☐ 雇用契約で営業秘密保持を定めている
	☐ 秘密保持契約を締結している（秘密保持範囲と守秘期限を定めている）
	☐ 守秘義務に違反した際の懲罰規定が明記されている
	☐ 退職者に対し競業避止義務を定めている
	☐ 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
	☐ 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
取引先管理	☐ 秘密保持契約を締結している
	☐ 秘密に該当する情報を明記している
侵害に備えた証拠確保	☐ 秘密度の高いエリアには監視カメラを設置している
	☐ メール送信記録、ウェブサイトの閲覧記録が確認できる

フォローアップ	□ 上記各項目について定期的に見直し、状況を把握している
---------	------------------------------

3. 管理体制整備のステップ 2ー営業秘密情報の洗い出し及び重要度の区分

(1) 営業秘密情報の洗い出し（☞ハンドブック P.6～13）

次に、保護すべき情報の洗い出しを行い、それらの重要度を区分する。営業秘密は、部署ごとに存在、保管されていることが一般的であることから、部署単位で洗い出しを行い、リスト化しておくといいだろう。参考までに、営業秘密の典型例を図 2 に示すが、そこに列挙したものはあくまで一例であり、上述したように、法律上の定義では、技術情報、経営情報に限られない。



（図 2）営業秘密の典型例

そして、リスト化の際にポイントとなるのが、項目として列挙する秘密情報の「粒度」である。粒度が大きすぎてしまうと（例えば「設計図」、「金型」等）、後述する重要度の区分を適切に行えない可能性がある。また、同一の製造工程に関する情報でも、それがどのような形態で存在しているかによって、例えば、工程表のように、工場内に掲示されて使用される紙資料と、工程上の管理数値などの電子データとして蓄積されている情報とでは、管理の具体的な手法は異なってくるから、少なくとも形態によって分類されるように粒度を設定する必要があるだろう。

いずれにしても、最も重要なのは、漏れなく秘密情報を把握することであり、

この点の考え方は当然、日本と変わらないので、ハンドブックの該当箇所も是非、参考にして頂きたい。

(2) 重要度の区分（☞ハンドブック P.14～16）

営業秘密の管理には、システム導入費用などの経済的コスト又は監視や管理等の担当業務の増加による人的コストを要することがほとんどであり、しかも、管理の結果として、業務上、多少の不便を生ずる場合も少なくない。したがって、すべての秘密情報に対して、厳格な管理ルールを適用すると、業務に支障をきたしかねない。

そこで、各情報の重要度に応じて管理するべく、洗い出した営業秘密について、重要度別に分類する。重要度の区分は、基本的には、その情報の価値に基づき判断することになると考えられるが、ハンドブックの該当箇所の記載も参照されたい。

(3) 特許

営業秘密管理に関連して、技術などを自社内に秘匿する又は特許権などの独占的排他権を実施するクローズ・モデルの知財戦略に加え、広く公開する又は他社にライセンスを付与するオープン・モデルの知財戦略を、上手に組み合わせていくことが昨今は重要である。

したがって、社内の情報について、営業秘密情報の洗い出し・重要度の区分を上述のとおり行ったらうえて、いずれの範囲までを営業秘密として秘匿・保護し、いずれの範囲から産業財産権として登録していくかという戦略を練ることも重要である。

なお、ベトナムの特許制度について、留意すべき点を以下で簡単に述べる。

ベトナムでは、第一国出願義務がある（知的財産法第7条、政令122/2010/ND-CP号第23条）。すなわち、ベトナムで生じた発明については、発明者がベトナム企業か外資系企業かにかかわらず、ベトナムで第一国出願をしない限り、ベトナムでの保護を受けることはできない。また、国防等の観点から、秘密特許と認定すべきかの審査期間（出願日から6か月）が経過してから、外国において特許出願を行うことができる（ただし、当局により秘密特許と認定された場合には、外国での特許出願はできない。）。

一方、ベトナム人又はベトナム企業が発明した場合には、発明がなされた場所にかかわらず、ベトナムで第一国出願をする義務がある。秘密特許と認定された

場合には、当局の許可を受けて、秘密特許制度を有する外国への特許出願が可能となる。

もともと、秘密特許の具体的な認定手続についてはまだ定められておらず、現時点で秘密特許を登録することは事実上困難である。

また、職務発明についてその特許権の帰属が問題となるが、ベトナムでは、当事者の別段の合意がない限り、原則として「資金及び物的施設を創作者に対し職務割当又は雇用の形態で投資した組織又は個人」に帰属すると定められており（知的財産法第 86 条第 1 項第 b 号）、職務発明の場合の特許権は原則として使用者に原始的帰属すると解される。

ただし、創作者に対して、最低でも以下の報酬額を支払うことが義務づけられている（知的財産法第 135 条第 2 項）。

- (i) 所有者が発明又は工業意匠又は回路配置の使用から得た収入の 10 パーセント
- (ii) 発明又は工業意匠又は回路配置のライセンス付与による各支払時に、所有者が受領した金銭合計額の 15 パーセント

4. 管理体制整備のステップ 3ー管理体制の整備

(1) 担当部門/担当者の設置（☞ハンドブック P.95～106）

管理体制の整備に当たり、まず必要なのは、営業秘密管理の担当部門、担当者の設置、配置である。中小企業に限らず、大企業であっても、ベトナム拠点での体制整備はほとんどなされていないケースが散見されるが、営業秘密管理を指揮する立場の駐在員等の担当者がいないことが、その理由の 1 つとなっているように思われる。筆者らの支援事業や他の業務の中での経験では、営業秘密管理の担当者はもとより、知的財産や法務の担当者をベトナムの製造拠点に配置している企業はごく少数に過ぎない。そもそも、日本の本社においても、ベトナムの特許権や商標権を担当する知的財産部員はいても、ベトナムの営業秘密管理を考える担当者が配置されているという例はほとんど聞かない。営業秘密管理体制の整備には、知的財産、人事・労務、情報セキュリティ、法務等、様々な視点からの横断的な検討が必要であり、従来型の一般的な企業の縦割り組織にはなじみにくいという性質があることや、営業秘密管理のような予防法務については、後回しにされがちであることが関係しているかもしれない。

いずれにしても、営業秘密の管理・保護に係る担当者が不在、又は不明確であることによって、管理体制の整備が進まないままになっていたり、管理体制自体は整備されていても、運用のチェック等の日常的な対応が手薄になってしまうことは、容易に想定される。少なくとも、基本的な管理体制を整備し、現地での運用がある程度軌道に乗るまでは、日本本社での営業秘密管理の状況を理解している人員が、ベトナム拠点での指揮、指導を行うのが望ましいかもしれない。

その上で、営業秘密管理を担当する専門の部署を設置、又は人員を配置できれば理想的ではあるが、運用上、より重要なのは、営業秘密が存在する各部署において、営業秘密管理の担当者を決めることである。管理体制の構築にあたって行う営業秘密の洗い出しや重要度の区分は、基本的には部署単位で行われるものであり、また、営業秘密の漏えい防止のためには、整備した管理体制の運用を適切に維持していくことが必要であるところ、かかる運用状況のチェックも、部署単位で行うことになるからである。

なお、各部署に担当者を設置した場合は、担当者を構成員として、営業秘密管理のための横断的な委員会を組織するなどして、定期的に会合の機会を設けて、情報共有（トラブル事例や管理上の工夫等）や、それに基づく運用の見直し等を議論することが望ましい。

(2) 従業員の管理

① 対象

正社員はもちろん、オフィス・工場内で業務に従事する派遣社員等が存在する場合には、それらの者に対する管理も必要である。すなわち、派遣元の会社との間の契約に、派遣社員の秘密保持に関する条項、自社の営業秘密研修を受講させる条項や、派遣社員による侵害が発生した場合に、派遣元会社に対して連帯責任を負わせる条項を含めることを検討すると良い。

② 秘密保持契約（☞ハンドブック P.48～50）

従業員管理の柱は、従業員に対して秘密保持義務を課すことである。その前提として、職務の遂行過程で創出されたノウハウ等が会社に帰属するものであることを、労働契約や秘密保持契約で明確に規定しておくこと。労働法においても、「雇用者は、労働者が法令の定めるところにより営業上の秘密又は技術上の秘密に直接関わる業務に従事する場合、営業上の秘密又は技術上の秘密の保護に関する内容及び期間並びに違反した場合の権利及び賠償について労働者との

間で書面により合意する権利を有する」という定めがある（労働法²¹第 21 条第 2 項）。

従業員との秘密保持契約のポイントは、以下のとおりである（参考書式 1、2 参照）。

- ・ 在職中及び退職後においても、秘密保持義務を課すこと（退職後の秘密保持について、入社時点で誓約させておくが良い）
- ・ 契約にて可能な範囲で、秘密情報を列举、特定しておく。ただし、どうしても契約上の文言では抽象的となり、各従業員が日常業務において、いかなる情報が秘密情報に当たるかが理解できていない結果、せつかくの情報管理規程がうまく運用されていないというケースが実際に散見される。そこで、部署単位で、具体的にどのような情報が秘密情報に当たるのか、認識を共有しておくとうい。
- ・ 退職時の秘密情報に関する資料等の返還義務を規定する。

③ 競業避止義務

ベトナムにおいて従業員に競業避止義務を課すことの有効性は、よく議論になる点である。

自由に職業を選択することはベトナムでも憲法において認められた国民の基本的な権利の一つであり（憲法第 35 条）、労働法においても、労働者には職業選択の自由があると規定されている（労働法第 5 条 1 項第 a 号）。このため、一般的に、労働者の職業選択の自由を一方的に制限することは、形式上労働者の同意が得られたとしても、労働者の権利を侵害する行為となりえる。また、労働法は、在職中であつても労働者の兼業を認める規定を置いており（第 19 条）、この規定には、兼職することとなる他社が同業であることや秘密保持を理由とする例外はない。

したがって、一般的には、在職中であつても退職中であつても、他社への就職を禁止する競業避止義務を従業員に課すことの有効性については疑問があると言わざるを得ないと考えられる。

しかしながら、以下に概要を紹介するとおり、期間の定めない競業避止義務を定めた合意書については職業選択の自由に反するとして無効とした裁判例もある一方で、退職後 12 か月間、同業他社、競合し得る他社、関連会社、取引先等に就職しないとする競業避止義務を定めた秘密保持契約が私人間の契約として有効であるとする裁判例もあることから、退職後の競業避止義務について労働者と合意することが必ずしも一律に無効となるとまではいえないように思われ

²¹ 法律 45/2019/QH14 号

る。

以上を踏まえると、明確な法律上の規定もなく判例の蓄積もないベトナムにおいて競業避止義務を退職者に課すか否かは判断が難しいところでもあるが、退職者がその有効性を争った場合には無効となる可能性又は違法に就業の機会を奪われたとして損害賠償を求められる可能性があることに留意しつつ、かかる義務を導入するという判断もあり得る。その場合も、日本での議論同様、制限の期間・範囲（地域・職種）や一定の代償措置を設けるなど内容が合理的といえるものになるよう慎重に検討・対応する必要があると考える（参考書式3 参照）。

また、競業避止義務を締結した場合、必要に応じて、調査会社を利用するなどして、退職者の義務の履行状況を調査することも考えられる。

競業避止義務に関する裁判例

○競業避止義務・契約の有効性を否定した裁判例

基本情報	裁判所/ 審級	ホーチミン市人民裁判所/第二審
	事件番号	第 420/2019/LD-CT 号
	判決年月 日	2019 年 5 月 15 日
	使用者	A 社
	労働者	B
経緯	• B は、2012 年 11 月から 2017 年 8 月の間、当初は 3D 設計スタッフ、その後は画像編集・販売スタッフとして A 社で勤務していた。2016 年、B はグループリーダーに昇進し、雇用契約の更新とは別に、A 社との間で別途秘密保持・知的財産権・競業避止に関する合意書（以下「本件合意書」という。）を締結した。本件合意書には、B が A 社退職後に A 社の秘密情報を不正使用しないこと、A 社の同業他社への就職をしないこと（期間制限無し）が B の義務として規定されていた。 • 2017 年 8 月、B と A 社との間の雇用契約が終了し、2017 年 10 月、B は C 社と雇用契約を締結した。それを確認した A 社は、C 社が A 社の同業他社に該当するとして、B に対し C 社を退職するよう要求する警告状を送付したが、B はその要求に応じなかった。そのため、A 社は、B に対し、本件合意書に基づき C 社を退職するよう請求する訴訟を提起した。 • 第一審では、裁判官は、憲法第 35 条第 1 項、2012 年労働法第 5 条第 1 項	

	第 a 号、第 10 条第 1 項、雇用法第 4 条第 1 項、第 9 条第 6 項に定める労働者の職業選択自由の原則に基づき、本件合意書の有効性を認めず、A 社の請求を認容しなかった。 • 第一審の判決に対して不服がある A 社は控訴を申し立てた。
裁判所の認定	ホーチミン市人民裁判所は、おおむね次のような理由を述べ、A 社の申立てを棄却した。 • C 社が A 社の競合とはいえないこと（C 社が登録した事業内容（コンピュータコンサルタント及びコンピューターシステム管理）は、A 社の事業内容（コンピュータープログラミング）とは異なるものであり、また、C 社が A 社の同業他社と証明できる適切な証拠がなかった。）。 • 第一審裁判所の判決のとおり、本件合意書の内容は労働者の職業選択の自由に反するため、有効とは認められない。 • B と C 社との間の雇用契約は適法に締結されている。

○競業禁止義務・契約の有効性を肯定した裁判例

基本情報	裁判所/ 審級	ホーチミン市人民裁判所/第一審
	事件番号	第 755/2018/QĐ-PQTT 号
	判決年月 日	2018 年 6 月 12 日
	使用者	X 社
	労働者	Y
経緯	• 2005 年 10 月、使用者である X 社は、労働者 Y を人事採用部部長として採用することとし、雇用契約とは別に、秘密保持契約を締結した。その秘密保持契約においては、退職理由の如何を問わず、(i)退職後 12 か月間、Y は同業他社、競合し得る他社、関連会社、取引先等に就職することを禁止すること（以下「本件競業禁止条項」という。）、及び(ii)それに違反した場合の損害賠償責任が規定されていた。 • 2016 年 11 月、Y は X 社を退職した。2017 年 10 月、Y が同業他社に就職していることを確認した X 社が、秘密保持契約において紛争解決機関として合意していたベトナム国際仲裁センター（VIAC）に仲裁を申し立て、Y に対し、本件競業禁止条項の違反を理由とする損害賠償を請求した。 • 仲裁では、X 社の Y に対する損害賠償請求を認容する判断が示された（ただし、仲裁判断の内容は非公開が原則とされているため、それ以上の詳しい理由付けなどは明らかにされていない。）。	

	• 仲裁判断が示された後、Y は、(a)本件のような労働紛争には、仲裁機関である VIAC の管轄は及ばない、(b)そもそも、本件競業避止条項は、労働者の職業選択の自由に違反するものであり無効であるとし、ホーチミン市人民裁判所に対し、VIAC の仲裁判断を取り消すことを求める民事非訟を申し立てた。
裁判所の認定	裁判所は、まず(a)を否定して労働紛争についても仲裁の管轄は及ぶとした上で、(b)について、おおむね次のような理由を述べ、X の申し立てを却下した。 • 民法第 3 条第 2 項は「個人及び法人は、自己の意思で民事の権利及び義務を確立し、履行し、消滅させる。法律の禁止事項に反さず、公序良俗に反しないすべての約束及び合意は、各当事者に対する拘束力を有し、他の主体により尊重される」と規定している。 • 秘密保持契約を締結する時点で、Y は民事行為能力を有し、契約に定める権利義務を十分に理解した上で任意に契約を締結した。すなわち、秘密保持契約は、X 社と Y との自由意思に基づいて締結された。 • したがって、X 社と Y との自由意思により締結された秘密保持契約の内容は合法であり、本件競業避止条項も労働者の職業選択の自由を制限するとはいえない。
備考	2010 年 12 月 10 日付の南部ロンアン省ドゥックホア郡地方裁判所第一審判決（09/2010/LD-ST 号）においても、上述の裁判と同様の考え方を取り、競業避止条項は当事者の自由意思によって締結された合意であるため、職業選択自由の原則に違反するものではなく、有効かつ拘束力があると判断している。

④ 私物携帯電話/SNS 対策

ベトナムで営業秘密管理を考える上で、特に重要となるのが、社員、特に、製造現場内での社員の携帯電話の管理と、Zalo²²や Facebook をはじめとする SNS の使用の管理である。ベトナムでは、携帯電話及び SNS が業務上用いられることが多く、その普及率は極めて高いと推測される。

しかしながら、営業秘密は、視覚的に把握できる情報が多いところ、私物の携帯電話は、即時にかかる情報を取得することができ、しかも、一旦、社外に出してしまえば、会社のコントロール圏外に流れ出てしまうという問題点がある。また、Zalo や Facebook といった SNS は、通常、私物携帯電話のアプリとして使用されるため、携帯電話で撮影された画像データなどの流出リスクが高い。

²² ベトナム企業である VNG Corporation が開発したモバイルメッセージアプリ。ベトナム国内で広く普及している。

したがって、私物の携帯電話及び SNS の業務上の利用は、できる限り制限するのが理想的である。

他方、ベトナムでは、日本人の想像をはるかに超えて携帯電話が生活に密着しており、また、顧客であるベトナム企業が SNS での連絡を希望してくるケースも多いため、全面的にこれらの使用を禁止することは、現実的ではなく、従業員からの強い反発も予想される。

そこで、まずは、自社の実態（携帯電話、SNS がどこまで業務上利用されているのか、また、どこまでこれを認める必要があるのか）を把握した上で、管理の方針を決めることが必要となる。

■日系企業の管理の実例—携帯電話利用管理

(a)社用携帯電話の貸与と私物携帯電話の持ち込み禁止

A 社では、工場内で撮影されたと見られる新製品の画像が発表前に流出する事例が数件発生しており、その再発防止が必要とされていた。

流出した画像は携帯電話のカメラで撮影されたものと思われたため、A 社は、工員以外の従業員に、社用の携帯電話を貸与することとし、その代わりに以下の措置を講じた。

- ・私物のカメラ付き携帯電話の社内への持ち込みは全面禁止とした。
- ・カメラ機能が付いていない私物の携帯電話は社内に持ち込むことはできるが、業務での使用は禁止した。
- ・貸与する社用携帯電話にはシールを貼付し、一見して社用であることが分かるようにした。

これらの措置により、社内で私物の携帯電話を使っている場合には直ちに違反行為であることが明確になり、また社内で使用される携帯電話は会社の所有物であるため、必要に応じてその使用履歴等の確認が行えるようになった。これらの措置が取られた後は、社内の画像の流失事件は発生していないとのことである。

(b)カメラの使用ルール

B 社では、工場内に設置された機械やそれらを用いた工程等も重要な営業秘密を構成しており、工場内部それ自体が秘密情報というべき状態であったため、工場内での写真撮影は全面的に禁止していたが、業務上の目的で撮影する必要が生じることもあった。

そこで、B 社では、以下の措置を講じた。

- ・写真撮影を行う場合には、会社が所有するカメラ及び SD カードを用いることとした。

- ・撮影の際には事前に工場内の営業秘密管理担当者等の許可を得て、その旨が明記された腕章を付けて撮影を行うべきこととした。
- ・撮影後は、データは SD カードから速やかに削除し、保管が必要であれば、当該部門のフォルダに速やかに移置することとした。

(c)携帯電話の使用制限

大規模な工場を運営する C 社では、従業員数が多いため、携帯電話の持ち込みを禁止しても保管場所の確保や盗難の防止が難しく、従業員からの反発も予想されたため、携帯電話の持ち込み禁止は実施していない。その代わり、最も情報漏えいのリスクが高いのは社内でのカメラの使用であると思われるため、社内では携帯電話のカメラにシールを貼付することをルール化し、徹底している。

⑤ ノウハウの有形化

製造現場の従業員は、基本的には、日々、同一の製造工程を担当することになるから、担当工程において、新たなノウハウを生み出すことも多いと思われる。しかし、こうした新たなノウハウが、従業員の頭の中にとどまっている限りは、本来は会社の資産として管理されるべきものも、その従業員の退職とともに流出し、転職先の競業企業で利用されかねないし、そもそも、それを自社の営業秘密として主張することも困難と考えられる。

こうした事態を防ぐため、まずは、従業員と締結する秘密保持契約において、職務上、創出されたアイデアなどは、ノウハウも含めて、会社帰属とすることを約定すること、その上で、ノウハウについて、評価、褒章の対象とするなどして²³、積極的に開示させる仕組みを作り、もれなく有形化して、会社の知的財産として管理することが重要となろう。

⑥ 研修（☞ハンドブック P.46～48）

ベトナムでは、まだまだ営業秘密保護や知的財産権の保護に関する意識が従

²³ 知的財産法においては、特許、意匠及び回路配置の職務発明に関して、創作者に対して、最低でも以下の報酬額を支払うことが義務づけられている（知的財産法第 135 条第 2 項）。

(a) 所有者が発明又は工業意匠又は回路配置の使用から得た収入の 10 パーセント

(b) 発明又は工業意匠又は回路配置のライセンス付与による各支払時に、所有者が受領した金銭合計額の 15 パーセント

知的財産として登録されないノウハウ等については、かかる法定の報酬支払義務まではないと解されるが、上記報酬額に準じた扱いを当事者間で取り決めることで、知的財産の有形化を推進することに繋がると考える。

業員に根付いているとまでは言い難い状況である。したがって、ベトナムにおける従業員管理においては、従業員の啓発活動としての研修も極めて重要である。特に、会社の営業秘密の侵害は解雇を含めた懲戒処分の対象にもなるということ、また、会社が大きな損害を受ける可能性があることを理解させることが、まずは必要であろう。

さらに、営業秘密管理に関する社内規程等の導入の際には、内容を周知させるために、研修を開催することも必要である。

■日系企業の管理の実例—研修の実施

A社は、数年前に営業秘密管理に関する社内規程を整備していた。しかし、その後社内規程の違反事例が散発するようになった。違反者に対する聴取を行ったところ、従業員の入れ替えもあり、社内規程の内容を知らない従業員が増えているように見受けられた。そこで、A社では以下の方法で営業秘密管理に関する社内研修を行った。

- ・年1回、社内の情報管理委員会が資料を作成し、各部署の営業秘密管理担当者がその資料を使って各部署で研修を行うこととする。
- ・研修終了時には小テストを行う。小テストで規定点数以上を取れない従業員については規定点数以上となるまで再テストを行う。
- ・テストに合格後、研修を受けその内容を理解したこと、及び関連社内規程を遵守することについての確認書に署名をしてもらう。

この研修を行うようになって以降は、営業秘密管理の重要性の認識が高まり、違反事例は劇的に減少した。また、違反者に対しては、確認書を見せることで、社内規程を知らなかったなどの言い逃れを許さず反省を促すことができるようになった。

⑦ 退職時の対応（☞ハンドブック P.55～62）

ベトナムでは、一般的に、会社への帰属意識が日本と比べると高くはなく、また、転職に対しても、むしろポジティブにとらえられている面がある。こうしたことを背景として、ベトナムでは人材流動性が相対的に高く、従業員の退職に伴う営業秘密漏えいのリスクも、それだけ高いといえる。

このため、退職時に営業秘密をすべて返還させることはもちろんだが、退職の申し出があった時点で、当該従業員に対する監視を強化する（社用メールの送受信履歴・状況の確認、社内システムからのダウンロード状況の確認等）、営業秘密へのアクセスを制限するなど、早めの対策が必要である。

また、退職時の営業秘密の返還等について、誓約書を提出させることも考えら

れるが、退職時には、サインを拒否するなどの可能性があるため、上述のように、予め雇用契約で誓約させておくとともに、退職のための事務的な書類と誓約書を組み合わせて、社員が自然にサインしやすくなるなどの工夫が考えられよう。

⑧ 職場環境の整備（☞ハンドブック P.53～54）

従業員の退職に伴う営業秘密漏えいリスクをいかに低減させるかを考えると、良好な職場環境を整備し、人材の流出を防ぐという視点も重要である。具体的には、従業員の成果を公平に反映した賃金体系を基礎とする待遇面の整備、改善を柱としつつ、従業員が平日の大半の時間を過ごすコミュニティとなっていることを考慮すると、いかに就業時間、休憩時間を気持ちよく過ごせるか、といった観点からの物理的、対人環境の整備、改善も重要な視点となろう。

こうした職場環境の整備は、営業秘密の漏えいを物理的に防ぐものではなく、効果としては間接的ではあるが、社員の長期定着につながり、営業秘密漏えい対策のためのルールを導入の際に、社員の理解が得られやすくなるという傾向があるようである。

(3) 執務室の管理

① 物理的なアクセス制限（☞ハンドブック P.76～77）

執務室の入り口には、ID カード認証などにより、物理的にアクセスを制限すべきである。また、建物の構造上、例えば、外部来訪者も往来可能な廊下などから執務室内が丸見えとなっているケースもよく散見される。執務室の窓にはブラインドやロールカーテンなどを設置することを検討すべきである。

② 紙資料の管理（☞ハンドブック P.29～30、P.50～51）

紙資料の秘密情報については、それぞれに「Confidential」等、秘密情報であることを示す表記を行うとともに、鍵付きのキャビネットで保管することが望ましい。営業秘密への不必要なアクセスを防ぐべく、営業秘密ではない一般書籍などとはキャビネットを分けるべきである。特に重要度の高い図面等については、専用の保管室を設け、全体を施錠し、図面の持ち出しを記録管理（持出し/返却日、使用者名と、管理担当者の確認チェック等）することを検討しても良い。アクセスへの手間をかけさせることで、自ずとアクセス制限を強化することになるからである。

■日系企業の管理の実例—印刷の管理

(a)プリンターの運用

A 社では、社内のプリンターがネットワークでつながっており、どの PC からもどのプリンターにでも印刷することができるようになっていたところ、間違ったプリンターに印刷を出してしまい、印刷物が放置されるという事態が多く発生し、情報漏えいのリスクがあった。そこで、A 社が、各従業員が持っているセキュリティカードをプリンターにかざさないと印刷物が印字されないというシステムを導入したところ、印刷物の放置がなくなったばかりか、無駄な印刷物も減少し、コスト低減という副次的な効果も得られた。

(b)機密情報の印刷禁止

B 社では営業秘密を重要度に応じて 3 段階に区分し、そのうち最重要に区分された情報については、PC からのプリントアウトができないようにシステム上設定されている。

③ 印刷物の管理

まず、電子データで存在する営業秘密情報は、必要最小限の範囲でのみ、印刷可能とすることが望ましい。業務上、印刷することが必要な場合には、印刷物のその後の管理手法（例えば、個人の鍵付き引き出し内で管理し、不要になったら直ちにシュレッダーで廃棄、自宅等への持ち出しの禁止等）についても、社内ルール化しておくとういだろう。

また、裏紙を利用している企業も多いと思われるが、営業秘密保護の観点からは、できれば裏紙利用を禁止したいところである。

(4) 生産現場の管理

① 物理的なアクセス制限

執務室同様、製造現場の入り口には ID カード認証などにより、物理的にアクセスを制限すべきである。入館者の登録、入館証の配布、立ち入り先の制限等をマニュアル化して行うことも考えられる（参考書式 5 参照）。

■日系企業の管理の実例—工場におけるアクセス制限

A 社では、商談や工場見学に訪れた外部の人が、社内のどこに立ち入ることができるかについての明確なルールが存在していなかった。

そこで、支援事業において、A 社に対しては以下のような対策を採ることを提案した。

- ・工場の入り口から最も近いエリアに、商談などに訪れた人が立ち入る社外

許可エリアを設置する。

- ・社外許可エリアとそれ以外のエリアとの境界には、施錠可能なドアやゲートを設置して物理的にアクセスを制限する。
- ・工場見学者など、外部の人が社外許可エリア以外のエリアに立ち入る場合には、受付において氏名・所属などを記載してもらって営業秘密管理担当者の許可を得るとともに、許可を有することが一目で分かる腕章を付けてもらう。また、スマートフォンやカメラなどは専用の透明の袋に入れて首から提げてもらい、スマートフォンのカメラ部分には剥がすと貼れないシールを貼付してもらうことにする。

② 製造機械、製造マニュアル、工程表等

製品や製造工程によっては、製造機械の構造やパネル表示、あるいは、製造機械自体が営業秘密に該当するという場合もある。このような場合、特に外部者が工場見学を行う場合等には、必要な部分をフィルムシートなどで覆うことを検討すると良い。

工場内では、稼働中、製造マニュアルや図面などが参照されることが多いと思われるが、特に、工場入り口にアクセス制限がかけられている場合、工場内でのこうした秘密情報の管理がおろそかになりがちである。工場内の営業秘密情報も、執務室と同様、未使用時には鍵付きのキャビネットなどに保管して管理すべきである。

また、営業秘密を含む製造工程表などを工場内のホワイトボードなどに掲示することも多いと思われるが、これらの掲示物にも「Confidential」等の表記は必要である。こうした工程表などを掲示したホワイトボードなどは、外部者の工場見学時には、見学ルートからは見えない位置に移動、又は目隠しすることも検討すべきである。

③ 金型

工場内には、金型のように、現物として存在する営業秘密もある。金型は一般的には、大型で持ち運びが困難であるが、それ故に、管理を怠りがちである。小型のものは施錠管理できるようにした上で、金型管理の担当者により、使用、保管状況を管理するとともに、金型保管エリアでは、携帯電話の持ち込みを禁止とすることなどを検討すべきである。

④ 不良品等の廃棄

特に BtoB 製品の場合、製品を構成する部品を含め、製品実物が営業秘密を構成する場合もある。こうした場合、製造過程で発生した不良品等の処分にも注

意する必要がある。自社内で完全廃棄するのが最も低リスクであるが、それが困難であり、外部業者に廃棄を委託する場合には、廃棄品の引き取りまで、それらが持ち出されることのないように、施錠管理し、可能な限り、容易に組み立てできない状態にまで分解等した上で引き渡しを行い、必要に応じて廃棄に立ち会う、といった対応が考えられる。もちろん、廃棄を委託する外部業者との間では、秘密保持契約の締結が必要である。

自社独自の仕様を指定して、他社に製造委託を行う場合も同様に、製品を構成する部品を含めて、製品実物が自社の営業秘密を構成し得るので、この場合には、製造委託の際に、不良品等廃棄について、上記の観点から、廃棄方法を指定する、監査項目に廃棄状況を含めることも検討すると良いだろう。

⑤ 特に重要度の高いエリア

工場内で特に重要度の高いエリアについては、アクセス制限を二重とすること等、管理の強化を検討することが望ましい。具体的には、別室化やゲート設置により、立入可能な人員をさらに限定することがメインとなるが、重要度の高いエリア内の機械等が、他のエリアから容易に見えてしまうことのないように、ブラインドの設置等、エリアの境界における視覚的なアクセス制限もあわせて検討する必要がある。

■日系企業の管理の実例—重要度に応じたゾーニング

A 社では、営業秘密を保護する重要度の高さに応じて工場内を 4 つのエリアにゾーン分けしており、それぞれのエリアに入ることができる従業員を ID カードで識別し、管理している。最重要のレベル 4 のエリアには、最初のドアを閉めないと次のドアを開けることができない二重扉を設置し、レベル 3 のエリアには入室記録がないと退出できないセキュリティシステムを設置している。また、工場の外周にはフェンスセンサーを設置し、工場内の要所にはセキュリティカメラを設置している。

(5) 取引先の管理

① 対象

第 1 章で述べたとおり、取引漏えい型の典型は、下請け又は顧客企業からの漏えいである。日本企業の場合、どうしても顧客に対して遠慮する傾向があり、特に、受注前に秘密保持契約を締結することをためらいがちであるが、むしろ顧客のベトナム企業は日本企業が考えるほど気にしていないことも多く、遠慮は不要である。

下請け、顧客のほか、ライセンサー（特許権等のライセンスにおいて、その特許技術の実施に必要なノウハウ指導を行う場合等）や、不良品等の廃棄物処理業者等との間でも、秘密保持義務を課すことが必要である。

② 秘密保持契約

取引先管理の柱は、契約にて秘密保持義務を課すことである。製造委託契約など、当該取引の基本契約中に秘密保持条項を含めるほか、別途、秘密保持契約を締結することも考えられる。秘密保持条項の主なポイントとして、以下が挙げられる（参考書式4参照）。

- ・ 何が秘密情報に当たるかを可能な範囲で特定すること。
- ・ 取引終了時に、秘密情報の返還又は破棄（破棄の場合は、破棄したことを証明する書面を提出させる）させること。
- ・ 特に、下請けやライセンサーに対しては、必要に応じて、情報管理についての監査・指導を受け入れること。

③ 工場見学（☞ハンドブック P.77）

特に顧客との関係で注意が必要なのが、工場見学である。実際、ベトナム顧客企業の工場見学の際に、大勢で日系企業の工場に立ち入り、その中には本当に顧客の社員なのかよく分からない者が含まれていたという事例や、ベトナム顧客企業が、監査と称して、日系企業の工場見学の際に勝手に動画撮影を行ったという事例などが発生している。こうした事態を防ぐべく、外部の者の工場見学の際には、以下の対策を検討すべきである。

- ・ 事前に、身分証明書の提示を求めること、及び、提示がなければ入構できない旨を予め通知し、来訪者の人数、氏名を事前に正確に把握すること。
- ・ 工場見学の前に、秘密情報を漏えいした場合には損害賠償を追う旨明記された来訪者受付表に署名させること（参考書式5参照）。
- ・ 工場見学者用のロッカーを設置し、携帯電話等を含む手荷物をすべて預かること。また、その旨を予め通知しておくこと。
- ・ 携帯電話のカメラシール（携帯電話のカメラレンズ部分に貼付し、はがしたことが分かるシール）の活用。
- ・ 予め監査場所・見学者の動線を決めておき、営業秘密は目隠し等対応すること。

④ 取引先の管理体制のアセスメント（☞ハンドブック P.64～65）

取引先との間で秘密保持契約を締結したとしても、相手方のコンプライアンス意識が不十分であったり、あるいは、社内での情報管理体制がずさんであるような場合は、秘密情報の漏えいを防ぐことは實際上難しい。そこで、可能な限り、取引関係に入る前に、相手方の信用調査などを行ったり、場合によっては、監査を行うなどして、秘密情報を開示するにふさわしいかを確認すべきである。上述したセルフチェックシートを活用し、管理体制を報告させたり、指導を行っても良いだろう。

■日系企業の管理の実例—取引先の管理

A 社では、従業員の工場内での携帯電話やカメラの使用を禁止していたが、工事業者などの従業員がルールを知らずに携帯電話を使用するなどの事例が後を絶たなかった。そこで、A 社では、過去に従業員が工場内で携帯電話を使用したなどの違反行為があった業者については、それ以降の工事の入札などにおける評価の減点対象とすることを明記し、実際に適用したところ、それ以降工事業者などにおいてルールの順守が徹底されるようになった。

⑤ 共同開発の場合

ベトナム企業と共同で技術開発を行う場合、その過程で生み出された技術情報を、共有のノウハウとして保護する場合も考えられる。営業秘密の具体的な共有状況にもよると思われるが、基本的には、共有者がそれぞれ、合理的な秘密保護措置をとる必要があると考えられるため、共同開発契約では、営業秘密を共有とする場合に、相互に秘密保護措置を講じるべき旨の規定を盛り込むべきだろう。

なお、共同開発により創作された産業財産権について、「複数の組織又は個人が発明、工業意匠、回路配置の創作において共同して創作し又は投資した場合は、それら組織又は個人はすべて登録を受ける権利を有し、当該権利はそれらの者の合意によってのみ行使されるものとする」と知的財産法に定められているため（第 86 条第 3 項）、権利の帰属や行使方法について当事者間で明確に取り決めておくことも必要である。

5. 漏えい時の対応

(1) 漏えいの兆候（☞ハンドブック P.122～127）

漏えいの一般的な兆候は、漏えいのルートに応じて、以下のものが挙げられる

(いずれも、ハンドブックより抜粋。詳細はハンドブック参照のこと)。

① 従業員等による漏えいの兆候

- ・ (業務上の必要性の有無にかかわらず) 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
- ・ 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おそ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かか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 退職者による漏えいの兆候

- ・ 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
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 取引先による漏えいの兆候

- ・ 取引先からの突然の取引の打ち切り
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 |
|----------------------------------|

なお、従業員による営業秘密の漏えいについては、他の従業員からの内部通報によって、漏えいの兆候又は漏えい行為が発覚することもしばしば見受けられる。ベトナムでは、営業秘密漏えい以外の、従業員による不正行為（ビジネスパートナーからの不正なキックバックの授与、公務員への贈賄等）もいまだに多く、内部通報制度の導入も検討すべきである。

(2) 初動対応(☞ハンドブック P.127～130)

漏えいの兆候が見られた場合、速やかに事実関係を調査・確認すべきである。ここで注意しなければならないのは、できる限り、営業秘密侵害に関する証拠を、ベトナムの訴訟実務に即した形で適切に収集することが重要²⁴となるところ、内部調査にいたずらに時間をかけたり、あるいは、内部調査のやり方次第では、侵害が疑われる従業員に動きを察知され、証拠を隠滅される等のおそれがある、ということである。

したがって、漏えいの兆候が見られた場合には、証拠が散逸する前に、速やかに、現地の法律事務所等の専門家に相談し、専門の調査員による調査を行うことを検討すべきである。もっとも、ベトナムにおいては、営業秘密侵害行為への対応等に知見や専門性を有する法律事務所等は残念ながら、日本に比べると少ないと考えられ、法律事務所等の選定は慎重に行う必要がある。

かかる調査によって、営業秘密漏えいの実態を把握するとともに、侵害行為に関する証拠収集(漏えいしてしまった秘密情報の化体した PC や USB 等の所在、漏えいしてしまった秘密情報を用いて生産されたと思われる製品の所在の把握等)を図り、調査結果に基づき、取りうる手段から適切な手段を検討することが重要である。

(3) 民事訴訟

① 証拠の収集について

ベトナムでは、中国のように、原則としてすべての証拠に公証認証手続きを経ることは裁判上の証拠として認められる必要要件ではないが、一般的には、公証認証手続きを経た方が証明力は高いと判断される可能性が高いといえる。知的財産権侵害に関する紛争の場合、private bailiff office (văn phòng thừa phát lại) に現場

²⁴ この点は、後述する証拠保全制度を利用する場合も同様である。

を確認させ侵害事実があったことの認定書（certified written minutes、vi bằng）を作成し、侵害事実の証拠とする場合もある²⁵。

② 緊急保全措置

知的財産法には、(a)知的財産権者において回復不能な損害が発生するおそれがある場合、又は、(b)侵害の疑いのある商品及び関連証拠について、それらが適時に保全されないと、逸失又は破棄されるおそれがある場合、知的財産権者は、訴訟提起時又は提起後に、暫定的措置（証拠品の没収、差し押さえ、封印、所有権移転の禁止等）を講じるよう裁判所に請求できるとの規定がある（知的財産法第207条）。

具体的な内容・手続については、民事訴訟法に規定があり、証拠の収集、証拠保全、回復不能の損害の回避を目的として、当事者の申立てにより、裁判所が職権で、必要な証拠の保全措置（財産の譲渡禁止、差し押さえ等）を取ることができる旨定められている（緊急保全措置、民事訴訟法第111条、第114条）。実務上は、相手方が有している証拠の保全を申立てることが多く、この意味において、緊急保全措置は、相手方の手中にある証拠の収集手段と位置付けることができる。緊急保全措置の申立ての際には、当該証拠の意義と重要性を説明し、さらに原告自身で当該証拠を収集できないことや、相手方が特許権侵害行為を行っていることなどを具体的な証拠に基づいて説明することになる。したがって、侵害行為の立証に足りなくても、それを一定程度推認させる周辺的な証拠は必要になる。

どのような初步証拠によって、どこまで、侵害事実を疎明すべきかについては、ケースバイケースで判断すべきであり、そうした初步証拠の所在等も、初動の調査によって判明してくることから、やはり、初動の調査の段階から、証拠の収集方針も含めて、法律事務所等の専門家と相談すべきであろう。

もっとも、ベトナムの裁判実務においては、緊急保全措置があまり積極的に運用されている事例は少ないと推測され、強制力もないため有効に機能しうるかについては疑問が残る。

(4) 行政措置

知的財産権侵害についての行政措置は、主に、商標権侵害の場合に利用される

²⁵ ベトナムにおいては、知的財産権侵害について、科学技術省に属する知的財産研究所（VIPRI : Vietnam Intellectual Property Research Institute）による鑑定結果を証拠として用いることがある。この鑑定の対象に営業秘密侵害行為が含まれるかは法文上明らかではないが、運用上は、VIPRIにて営業秘密侵害行為の鑑定は行っていないようである。

ことが多く、営業秘密侵害に対する行政措置は、それらと比べるとかなり少ないと思われる。

特に、知的財産権侵害の場合にもっとも利用される機関である市場監督管理局は、(ケースバイケース、また、地域にもよるが、) 一般的には、技術の同一性の判断が必要となるケース、特に、技術内容が複雑なケースについては、対応が難しいとされることも少なくないと思われる。

行政措置は、このように、営業秘密侵害事案において、侵害証拠の収集手段の1つとも位置付けられ得るものであるが、侵害にかかる秘密情報の相手方における所在について、ある程度の蓋然性を以て、摘発の申立てを行う必要があるため、上記(2)で述べた調査によって、これらの証拠の存在をつかんでおくことが重要となる。

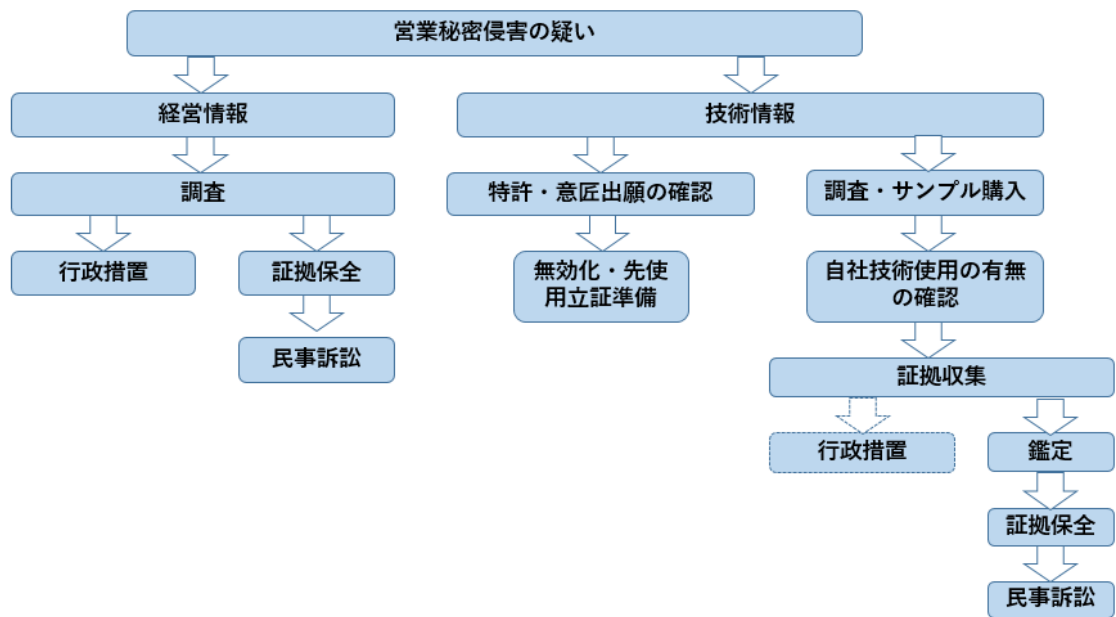
(5) 冒認出願の確認

特に、営業秘密が技術情報である場合、ベトナムでは、同情報をベースにして特許・意匠等が冒認出願されることもあり得る。このような冒認出願に対しては、無効審判を請求して、権利を無効化することが考えられる(知的財産法第96条)。

そこで、技術情報の漏えいが発生した場合には、冒認出願の有無を確認する必要がある。なお、冒認権利に基づき、自社又はその顧客が権利行使を受けるリスクもあり、これに備えて、先使用権立証のための証拠を整えることも、あわせて検討すると良いだろう。

(6) 対応フロー

以上の対応手段をまとめると、図3のようになる。最終的な法的手段の枠組みは、概ね、民事訴訟か行政措置かになるが、営業秘密が顧客リストなどの営業情報であるか、あるいは、設計図面や製法等の技術情報であるか、によって、準備すべき事項も変わってくる。いずれの場合においても、事実関係と証拠収集の可否、所在等について、早期に調査を行い、的確に対応手段を選択することが、重要となる。



(図3) 営業秘密侵害に対する対応フロー

参考書式

1. 就業規則における秘密保護関連規定の例

<日本語>

第○条（服務規律）

1. 従業員は、職場の秩序を保持し、業務の正常な運営を守るため、職務を遂行するにあたり、次の各号に定める事項を守らなければならない。
 - (a) 会社の施設、設備、製品、材料、電子化情報等を大切に取り扱い保管するとともに、会社の許可なく私用に使用しないこと。
 - (b) （以下略）
2. 従業員は、入退場に関し、次の各号に定める事項を守らなければならない。
（*1）
 - (a) 警備員から所持品の検査を求められたときは、応じること。
 - (b) 会社の許可なく、書類や社品を会社外に持ち出さないこと。
 - (c) （以下略）
3. 従業員は、従業員証を常時携帯し、入場のとき又は求められたときは、直ちに提示しなければならない。

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。

- (a) 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（*2）を、不正に開示したり、不正に使用したりしないこと。
- (b) 従業員は、在職中及び退職後[6 か月間/1 年間/2 年間]、会社と競合する他社に就職し、また競合する事業を営まないこと。（*3）
- (c) 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。）をすべて会社に返却すること。
- (d) （以下略）（*4）

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。

- (a) 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。
- (b) 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。
- (c) 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。
- (d) 会社の内外を問わず、業務に使用する端末において、会社が指定したものを除き、ファイル交換ソフト又は VPN 環境提供ソフトウェア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。
- (e) 会社の許可なく、私物の USB 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。
- (f) 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。
- (g) （以下略）（*5）

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。（*6）（*7）（*8）

- (a) 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ー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。
- (b) 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。
- (c) ウィルス感染等を予防するため、特定のホームページへのアクセスを制限すること。

第○条 懲戒 （*9）

従業員が就業規則の定めに違反した場合、違反の度合いに応じて、次の各号のいずれかに該当する懲戒処分を科される。

（中略）

解雇

従業員が次の各号の一に該当するときは、懲戒解雇される。

- (a) 窃盗、横領、賭博、故意の暴行、職場での傷害、薬物の使用、技術若しくは営業秘密の開示、又は会社の知的財産権の侵害

(以下略)

<ベトナム語>

Điều 〇. Kỷ luật làm việc

1. Để giữ gìn trật tự nơi làm việc và bảo đảm [hoạt động kinh doanh bình thường], khi tiến hành công việc, người lao động phải tuân thủ những điều quy định tại các mục sau đây.
 - a. Sử dụng và bảo quản cẩn thận các phương tiện, thiết bị, sản phẩm, tài liệu, thông tin điện tử của công ty, và không sử dụng cho mục đích cá nhân mà không được sự cho phép của công ty.
 - b. (Phần dưới lược bỏ)
2. Người lao động phải tuân thủ các vấn đề quy định tại các mục sau đây liên quan đến việc ra vào công ty.
 - a. Tuân theo yêu cầu khi được nhân viên bảo vệ yêu cầu kiểm tra đồ đạc mang theo;
 - b. Không mang tài liệu hoặc sản phẩm của công ty ra khỏi công ty khi chưa được công ty cho phép.
 - c. (Phần dưới lược bỏ)
3. Người lao động phải luôn mang theo thẻ nhân viên và xuất trình ngay khi đến công ty hoặc khi được yêu cầu.

Điều 〇. Điều khoản tuân thủ

1. Người lao động phải tuân thủ các nội dung quy định tại các mục sau đây.
 - a. Không tiết lộ trái phép hay sử dụng trái phép thông tin bảo mật của công ty bất kể là ở trong hay bên ngoài công ty, trong quá trình làm việc hay sau khi không còn làm việc cho công ty vì các lý do như nghỉ việc hoặc bị sa thải.
 - b. Người lao động không được làm việc cho các công ty là đối thủ cạnh tranh với công ty và không tiến hành các hoạt động kinh doanh mang tính cạnh tranh với các hoạt động kinh doanh của công ty trong quá trình làm việc và trong vòng [6 tháng/1 năm/2 năm] kể từ khi nghỉ việc.
 - c. Vào thời điểm nghỉ việc, trả lại cho công ty máy tính cá nhân và điện thoại di động được công ty cho mượn và tất cả các tài liệu (bao gồm giấy, dữ liệu điện tử và tất cả các phương tiện lưu trữ chúng) được nhận từ công ty.
 - d. (Phần dưới lược bỏ)

Điều 0. Sử dụng thích hợp thư điện tử, internet

1. Liên quan đến việc sử dụng thư điện tử, mạng nội bộ và mạng internet của công ty (sau đây gọi chung là "Internet"), người lao động phải tuân thủ các mục sau đây khi sử dụng máy tính cá nhân, điện thoại thông minh, điện thoại di động và các thiết bị thông tin và liên lạc khác (sau đây gọi chung là "Thiết Bị"), và phải nỗ lực duy trì môi trường mạng thông tin thích hợp và ngăn ngừa thiệt hại và rò rỉ thông tin nội bộ.

a. Không sử dụng Thiết Bị do công ty cho người lao động mượn vào bất kỳ mục đích nào khác ngoài công việc.

b. Không sử dụng thiết bị cá nhân cho mục đích công việc mà không có sự cho phép của công ty.

c. Vận hành và sử dụng đúng cách phần mềm chống vi rút do công ty chỉ định.

d. Không cài đặt phần mềm trao đổi tệp, phần mềm cung cấp mạng riêng ảo (VPN) và phần mềm khác có thể gây ra các vấn đề trong quản lý thông tin, hoặc phần mềm không liên quan đến việc kinh doanh của công ty vào các Thiết Bị được sử dụng cho công việc, bất kể là ở trong hay bên ngoài công ty, ngoại trừ phần mềm do công ty chỉ định.

e. Không kết nối phương tiện ghi như USB cá nhân hoặc đĩa cứng hoặc thiết bị cá nhân với Thiết Bị được sử dụng cho công việc mà không có sự cho phép của công ty.

f. Khi nhận được sự cho phép kết nối được quy định trong mục trên, cài đặt mật khẩu để người không có quyền truy cập không thể sử dụng.

g. *(Phần dưới lược bỏ)*

2. Nhằm sử dụng thích hợp Internet và quản lý thông tin bảo mật của công ty, công ty có thể áp dụng các biện pháp quy định tại các mục sau đây và các biện pháp được xem là cần thiết khác.

a. Truy cập các dữ liệu trong Thiết Bị mà công ty cho người lao động mượn hoặc được lưu trữ tại server của công ty, phân tích thông tin và kiểm tra lịch sử sử dụng Internet của mỗi người lao động khi cần thiết.

b. Truy cập nội dung thư điện tử công ty do người lao động gửi và nhận khi cần thiết.

c. Hạn chế quyền truy cập vào các trang chủ cụ thể để ngăn ngừa nhiễm vi rút.

Điều 0. Xử lý kỷ luật

Trường hợp người lao động vi phạm nội quy lao động thì tùy theo mức độ vi phạm sẽ bị xử lý kỷ luật lao động theo một trong các hình thức sau đây.
(Lược bỏ)

Sa thải

Người lao động sẽ bị áp dụng hình thức kỷ luật sa thải khi thuộc một trong các trường hợp sau đây:

- a. Trộm cắp, tham ô, đánh bạc, cố ý gây thương tích, sử dụng ma túy tại nơi làm việc, tiết lộ bí mật kinh doanh, bí mật công nghệ hoặc xâm phạm quyền sở hữu trí tuệ của công ty;
- b. (Phần dưới lược bỏ)

※本参考書式は、ハンドブック参考資料2の第1（P.149～151）をベースにしつつ、ベトナムの法令及び慣行に基づき、一部内容を修正し、注を加えたものである。

※ベトナムにおいては、10名以上の労働者を雇用する場合には、書面による就業規則を作成することが必要であり、営業秘密について規定することも義務づけられている（労働法第118条第2項第d号）。就業規則の内容については、労働組合の代表者又は労働者の代表者と事前の協議をすることとされており、協議の結果を添えて労働傷病兵社会局に登録する必要がある（労働法第119条）。また、雇用する労働者が10名未満である場合でも、就業規則を制定する必要があるとされている（書面によるべきことは要求されていない。）（労働法第118条）。

(*1) 従業員の入退場に関する規定として、下記のような定めを入れておく例もある。

- 会社の指示する手順を経て入退場すること。
Hoàn thành thủ tục ra vào công ty theo chỉ thị của công ty
- 日常携帯品以外の物品を携帯して入場しないこと。ただし、特に必要な場合は、会社の指示する手順をとること。
Không mang theo các vật dụng khác với các vật dụng hàng ngày khi ra vào công ty. Tuy nhiên, trong trường hợp đặc biệt cần thiết thì áp dụng thủ tục theo chỉ thị của công ty.

これに関連して、別途以下のような条項を設け、実効性を確保することも考えられる。

第○条（入場制限・退場命令）

従業員が次の各号の一に該当すると会社が認めた場合は、入場させず、又は退場させることがある。

- 入退場手続を行わないとき。
- 従業員証を所持していないとき。
- 警備員による所持品の検査に応じないとき。
- 業務外の事由で入場しようとするとき、又は終業後退場しようとしな
いとき。
- （以下略）

Điều ○. Hạn chế vào và buộc rời khỏi nơi làm việc

Nếu công ty nhận thấy người lao động thuộc vào bất kỳ trường hợp nào dưới đây, người lao động đó có thể không được vào hoặc bị buộc phải ra khỏi nơi làm việc.

- Không tiến hành thủ tục ra/ vào công ty
- Không mang theo thẻ nhân viên
- Không tuân theo yêu cầu khi bảo vệ yêu cầu kiểm tra đồ đạc mang vào
- Vào nơi làm việc vì những lý do ngoài công việc, hoặc không ra về sau giờ làm việc
- (Phần dưới lược bỏ)

(*2) 秘密情報の範囲や取扱方法が従業員等に対して明確化されることによつて、従業員等の予見可能性、ひいては、経済活動の安定性を確保することにあることから、情報管理規程等の中で、別途指定をする旨を就業規則内に定めることも考えられる。

(*3) 競業避止義務を従業員の遵守事項に含めることについては、就業規則登録時に当局から違法であると指摘されるリスク、又は紛争になった場合に無効とされるリスクはあることに留意する必要がある。従業員と競業避止義務に関する合意をすることについて認める裁判例がある一方、労働法 19 条は、在職中であっても労働者の兼業を認める規定を置いており、この規定には、兼職

することとなる他社が同業であることや秘密保持を理由とする例外はないことから、従業員に競業避止義務を課すことは職業選択の自由に反すると解される可能性があるからである。詳しくは、本マニュアル第2章4.(2)③を参照されたい。

(*4) 上記に掲げているものの他、従業員の秘密保持義務との関係では、下記の内容を遵守事項として規定することが考えられる。

- 会社の諸規則に違反する出版、又は講演などを行わないこと。
Không thực hiện việc các công việc như xuất bản hoặc giảng dạy trái với quy định của công ty.
- 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。(※)
Không đem thông tin bảo mật của công ty ra ngoài mà chưa có sự cho phép của công ty.
- 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。
Không được vào khu vực cấm ra vào, không đi vào khu vực không phải nơi làm việc của cá nhân vì những lý do khác ngoài công việc, hoặc sử dụng các phương tiện và khuôn viên của công ty mà không có sự cho phép của công ty.
- 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又は持分の売買又は譲渡を行わないこと。
Trong quá trình làm việc tại công ty và sau khi nghỉ việc, không sử dụng thông tin bảo mật của công ty mà mình biết được trong quá trình làm việc để trực tiếp hoặc gián tiếp mua, bán hoặc chuyển nhượng cổ phần hoặc phần vốn góp vào thời điểm trước khi thông tin này được công bố.

※上記のような規定を入れる場合、具体的な情報取扱い方法については、情報管理規程でより詳細に定めることが考えられる。ただし、就業規則において、詳細は情報管理規程を参照としておくと、労働傷病病社会局に登録する際に、そのような別途の内部規程を就業規則に紐付けるべきではないと指摘される場合があることには留意されたい。その場合は、最初から就業規則本文において、情報管理規程で規定すべき事項を盛り込んでおくという方法も考えられる。

(*5) 次のような条項を入れることも考えられる。

- 業務に関係のないホームページサイトにアクセスしないこと。
Không được truy cập vào các trang web không liên quan đến công việc.
- 会社が許可したもの以外のWebメール、ファイル共有サービス、オンラインストレージサービスの使用禁止
Cấm sử dụng webmail, dịch vụ chia sẻ chung tệp và các dịch vụ lưu trữ trực tuyến ngoài những dịch vụ được công ty cho phép
- 業務に利用する端末にはパスワードを設定し、当該パスワードを他人に開示しないこと。
Đặt mật khẩu cho Thiết Bị được sử dụng cho công việc và không tiết lộ mật khẩu này cho người khác.
- 業務に利用する端末の持ち出し、他人への貸与の禁止
Nghiêm cấm đưa Thiết Bị sử dụng cho công việc ra ngoài hoặc cho người khác mượn.

(*6) 本項を社内規定に導入するにあたって、案を策定し、事前に社内に徹底することが必要である。

(*7) 防犯カメラについては、あらかじめ従業員に通知し、必要に応じて協議を行った上で、次のような条項を入れることが考えられる。また、防犯カメラの設置等の責任者及びその権限も定めておくことが重要である。加えて、防犯カメラの設置等が適正に行われているかを監査又は確認することも重要である。

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
 - （以下略）
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
 - （以下略）

Điều ○. Lắp đặt camera an ninh

1. Công ty có thể lắp đặt camera an ninh và chụp lại hình ảnh ở những địa điểm quy định tại các mục sau hoặc khi xét thấy cần thiết cho mục đích phòng chống tội phạm và quản

lý thông tin bảo mật của công ty.

- Lỗi ra vào khu vực công ty
- Lỗi ra vào và bên trong phòng máy chủ
- (Phần dưới lược bỏ)

2. Công ty có thể truy cập và lưu trữ hình ảnh hoặc video từ camera an ninh trong các trường hợp quy định tại các mục sau hoặc khi xét thấy cần thiết.

- Khi có người xâm nhập bất hợp pháp
- (Phần dưới lược bỏ)

(*8) 就業規則以外で定めを置く場合を含め、本項に定めるような事項を実施するにあたっては、あらかじめ従業員に通知し、必要に応じて協議を行うことが望ましいと考えられる。また、その実施に当たっての責任者及びその権限も定めておくことが重要である。加えて、実施が適正に行われているかを監査又は確認することも重要である。

(*9) ベトナムでは、懲戒解雇できる事由は、以下の場合に限定され、会社が裁量で懲戒解雇事由を追加したり変更したりすることは原則認められない。もっとも、営業秘密の漏えい行為は、懲戒解雇事由の一つとされている（労働法第 125 条）。

- 労働者が、職場において、窃盗、横領、賭博、故意の傷害、麻薬の使用を行った場合
- 労働者が、使用者の経営の秘密・技術の秘密を漏えいし、知的所有権を侵害する行為、使用者の財産、利益に重大な損害をもたらす、あるいは特別重大な損害をもたらすおそれがある行為、又は就業規則で規定されるセクシャルハラスメントを行った場合
- 労働者が昇給期間延長処分又は降格処分を受け、その処分が消滅する前に再犯した場合。再犯とは、労働者が労働法第 126 条の定めるところにより処分が消滅する前に、再び処分を受けた規律違反行為を行うことをいう。
- 労働者が正当な理由なく、無断欠勤の最初の日から数えて 30 日間に合計 5 日、又は 365 日間に合計 20 日無断欠勤した場合。正当な理由があるとは、みなされる場合とは、天災、火災、自身又は親族が疾病に罹患し権限を有する診断治療所の確認を有する場合、及び就業規則に定めるその他の場合をいう。

2. 従業員の秘密保持に関する誓約書の例

<日本語>

秘密保持に関する誓約書

この度、私は、貴社に採用されるにあたり、下記事項を遵守することを誓約いたします。

第1条（在職時の秘密保持）

貴社就業規則[及び貴社情報管理規程]を遵守し、次に示される貴社の秘密情報（*1）について、貴社の許可なく、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。

- (a) 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貴社製品に関する情報
- (b) （以下略）

第2条（退職後の秘密保持）

前条各号の秘密情報については、貴社を退職した後においても、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。退職時に、貴社との間で秘密保持契約を締結することに同意いたします。

第3条（損害賠償）

前2条に違反して、第1条各号の秘密情報を不正に開示又は不正に使用した場合、法的な責任を負担するものであることを確認し、これにより貴社が被った一切の被害を賠償することを約束いたします。

第4条（第三者の秘密情報）（*2）

- 1. 第三者の秘密情報を含んだ媒体（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情報を記載又は記録するものをいう。）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秘密情報

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（以下「使用等」という。）させない、貴社が使用等するように仕向けない、又は貴社が使用等しているとみなされるような行為を貴社にとらせないことを約束いたします。

第5条（第三者に対する守秘義務等の遵守）（*2）

貴社に入社する前に第三者に対して守秘義務又は競業避止義務を負っている場合は、必要な都度その旨を上司に報告し、当該守秘義務及び競業避止義務を守ることを約束いたします。

（*3）

年 月 日

●●会社

代表者 _____

住 所 _____

氏 名 _____

<ベトナム語>

CAM KẾT BẢO MẬT

Tôi xin cam kết tuân thủ những điều dưới đây khi được tuyển dụng vào làm việc tại Quý công ty.

Điều 1. Bảo mật trong quá trình làm việc

Tôi sẽ tuân thủ nội quy lao động của Quý công ty [và các quy tắc quản lý thông tin của Quý công ty], đồng thời cam kết không tiết lộ hoặc sử dụng bất hợp pháp thông tin bảo mật dưới đây của Quý công ty khi không có sự cho phép của Quý công ty.

(a) Thông tin về sản phẩm của Quý công ty, bao gồm các thông tin như tài liệu kỹ thuật liên quan đến phát triển sản phẩm, quyết định về chi phí sản xuất và quyết định giá bán.

(b) (Lược bỏ)

Điều 2. Bảo mật sau khi nghỉ việc

Tôi cam kết rằng sẽ không tiết lộ hoặc sử dụng trái phép thông tin bảo mật tại Điều 1 ngay cả sau khi nghỉ việc tại Quý công ty. Tôi đồng ý rằng vào thời điểm nghỉ việc, tôi sẽ ký thỏa thuận bảo mật với Quý công ty.

Điều 3. Bồi thường thiệt hại

Trong trường hợp tôi vi phạm quy định tại hai Điều trên, tiết lộ hoặc sử dụng trái phép thông tin bảo mật quy định tại Điều 1, tôi xác nhận rằng sẽ chịu trách nhiệm pháp lý và cam kết sẽ bồi thường mọi thiệt hại mà Quý công ty phải gánh chịu do hành vi vi phạm nói trên.

Điều 4. Thông tin bảo mật của bên thứ ba

1. Tôi cam kết không và sẽ không sở hữu bất kỳ phương tiện nào (bao gồm tài liệu, bản vẽ, ảnh, bộ nhớ USB, DVD, ổ đĩa cứng, hoặc các phương tiện khác mô tả hoặc ghi lại thông tin) có chứa thông tin bảo mật của bên thứ ba.
2. Tôi cam kết rằng trong quá trình làm việc tại Quý công ty, tôi sẽ không để công ty tiết lộ, sử dụng hoặc đăng ký (dưới đây gọi là "sử dụng") bất kỳ thông tin bảo mật nào do bên thứ ba sở hữu mà không có sự đồng ý trước bằng văn bản của bên thứ ba đó, và sẽ không khiến Quý công ty sử dụng hoặc khiến Quý công ty bị xem là có hành vi sử dụng các thông tin nói trên.

Điều 5. Tuân thủ nghĩa vụ bảo mật đối với bên thứ ba

Trong trường hợp tôi có nghĩa vụ bảo mật hoặc không cạnh tranh với bên thứ ba trước khi vào làm việc tại Quý công ty, tôi sẽ báo cáo với cấp trên về việc này tùy từng thời điểm cần thiết và cam kết sẽ tuân thủ nghĩa vụ bảo mật và không cạnh tranh nói trên.

Ngày tháng năm

●●[Tên công ty]

Người đại diện_____

Địa chỉ _____

Họ và tên _____

※本参考書式は、ハンドブック参考資料2の第3の1（P.157～158）をベースにしつつ、ベトナムの法令及び慣行に基づき、一部内容を修正し、注を加えたもの

のである。

(*1) 情報管理規程等において、別途秘密情報の範囲が指定されている場合には、第1条各号に代わり、当該規程等を用いることも考えられる。

(*2) 特に転職者の入社時などに、他社の情報を意図せず侵害することを防止するという観点から、このような条項を設けることが望ましい。

(*3) 情報の帰属について、以下のような誓約事項を設ける例も考えられる。

なお、ベトナムでは、産業財産権の職務発明について、当事者の別段の合意がない限り、原則として「資金及び物的施設を創作者に対し職務割当又は雇用の形態で投資した組織又は個人」に帰属すると定められており（知的財産法第86条第1項第b号）、特許権は原則として使用者に原始的に帰属すると解される。

また、職務著作については、当事者の別段の合意がない限り、命名権・氏名表示権を除いて、使用者に原始的に帰属すると解される（知的財産法第39条第1項）。

第〇条（創出等した情報の報告及び帰属）

1. 貴社により秘密情報として指定された情報の範囲に含まれるものについて、その創出又は取得に関わった場合には、遅滞なくその内容を貴社に報告します。
2. 前項の情報については、私がその創出又は取得に携わった場合であっても、貴社業務上作成したものであることを確認し、当該情報の帰属が貴社にあることを確認いたします。また当該情報について私に帰属する一切の権利を貴社に譲渡し、その権利が私に帰属する旨の主張をいたしません。

Điều 〇 Báo cáo và quyền sở hữu thông tin được tạo ra

1. Tôi sẽ ngay lập tức báo cáo với Quý công ty nếu có liên quan đến việc tạo ra hoặc thu thập thông tin nằm trong phạm vi thông tin được Quý công ty chỉ định là thông tin bảo mật.
2. Ngay cả khi tôi có liên quan đến việc tạo ra hoặc thu thập thông tin quy định tại Khoản trên, tôi xác nhận rằng các thông tin đó được tạo ra trong quá trình làm việc tại Quý công ty và xác nhận rằng thông tin đó thuộc về Quý công ty. Ngoài ra, tôi sẽ chuyển nhượng cho Quý công ty tất cả các quyền của tôi đối với thông tin đó và sẽ không yêu cầu quyền sở hữu đối với các quyền này.

3. 退職時の秘密保持に関する誓約書の例

<日本語>

秘密保持に関する誓約書

私は、年 月 日付にて、一身上の都合により、貴社を退職いたしますが、貴社秘密情報に関して、下記の事項を遵守することを誓約いたします。

第1条（秘密保持の確認）

私は貴社を退職するにあたり、次に示される貴社の秘密情報に関する一切の資料、媒体等（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情報を記載又は記録するものをいう。）について、原本はもちろん、そのコピー及び関係資料等を、直ちに貴社に返還、消去又は廃棄し、その情報を自ら保有していないことを確認いたします。

- (a) 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貴社製品に関する情報
- (b) （以下略）

第2条（退職後の秘密保持の誓約）

前条各号に掲げる貴社の秘密情報を、貴社退職後においても、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。

(*1) (*2) (*3) (*4)

以上

年 月 日

●●会社

代表者 _____

住 所 _____

氏 名 _____

<ベトナム語>

CAM KẾT VỀ VIỆC BẢO MẬT

Vào ngày....tháng....năm...., tôi đã nghỉ việc ở Quý công ty vì lý do cá nhân, nhưng tôi cam kết sẽ tuân thủ những điều sau đây liên quan đến thông tin bảo mật của Quý công ty.

Điều 1. Xác nhận bảo mật

Tôi xác nhận rằng khi nghỉ việc tại Quý công ty, tôi sẽ ngay lập tức trả lại, xóa hoặc tiêu hủy bản gốc cũng như bản sao và các tài liệu liên quan của mọi tài liệu, phương tiện (là văn bản, bản vẽ, ảnh, bộ nhớ USB, DVD, ổ đĩa cứng và tài liệu, phương tiện khác ghi chép hoặc ghi lại thông tin) liên quan đến thông tin bảo mật của Quý công ty như được thể hiện dưới đây, đồng thời xác nhận rằng tôi không nắm giữ những thông tin đó.

(a) Thông tin về sản phẩm của Quý công ty, chẳng hạn như tài liệu kỹ thuật về phát triển sản phẩm, chi phí sản xuất và quyết định giá bán.

(b) *(Bên dưới lược bỏ)*

Điều 2. Cam kết bảo mật sau khi nghỉ việc

Tôi cam kết sẽ không tiết lộ hoặc sử dụng trái phép thông tin bảo mật của Quý công ty được nêu tại các khoản của Điều 1 kể cả sau khi nghỉ việc.

Hết

Ngày.... ThángNăm.....

Công ty ●●

Người đại diện _____

Địa chỉ _____

Họ và tên _____

※本参考書式は、ハンドブック参考資料2の第3の3(P.160～161)をベースにしつつ、ベトナムの法令及び慣行に基づき、一部内容を修正し、注を加えたもの

のである。

(*1) ベトナムにおいては、本マニュアル第2章4.(2)③記載のとおり、職業選択の自由に反するとして無効とした裁判例もある一方で、退職後12か月間、同業他社、競合し得る他社、関連会社、取引先等に就職しないとする競業避止義務を定めた秘密保持契約が私人間の契約として有効であるとする裁判例もあるところであり、退職後の競業避止義務について労働者と合意することが必ずしも一律に無効となるとまではいえないように思われる。

したがって、明確な法律上の規定もなく判例の蓄積もないベトナムにおいて競業避止義務を退職者に課するか否かは判断が難しいところでもあるが、退職者がその有効性を争った場合には無効となる可能性又は違法に就業の機会を奪われたとして損害賠償を求められる可能性があることには留意しつつかかる義務を導入するという判断もあり得る。ただし、退職後の競業避止義務については、その有効性が認められるためには、企業側の守るべき利益の存在を前提として、従業員の状態、地域的限定、競業避止義務の存続期間、禁止される競業行為の範囲、代償措置等について、具体的事情の下で合理的なものとなるように考慮する必要があるものと考えられる。

第○条(競業避止義務の確認)

貴社を退職するにあたり、退職後1年間、貴社からの許諾がない限り、次の行為をしないことを誓約いたします。

- (a) 貴社で従事した○○の開発に係る職務を通じて得た経験や知見が貴社にとって重要な企業秘密及びノウハウであることに鑑み、当該開発及びこれに類する開発に係る職務を、貴社の競合他社（競業する新会社を設立した場合にはこれを含む。以下同じ。）において行うこと
- (b) 貴社で従事した○○に係る開発及びこれに類する開発に係る職務を、貴社の競合他社から契約の形態を問わず、受注又は請け負うこと

Điều ○. Xác nhận nghĩa vụ không cạnh tranh

Tôi cam kết khi nghỉ việc tại Quý công ty, tôi sẽ không thực hiện những điều sau đây trong vòng 01 năm kể từ khi nghỉ việc mà không có sự cho phép của Quý công ty.

- (a) Tiến hành phát triển [...] và các nhiệm vụ phát triển mang tính chất tương tự tại các đối thủ cạnh tranh của Quý công ty (bao gồm cả trường hợp thành lập mới công ty cạnh tranh, dưới đây cũng sẽ được áp dụng tương tự), trên cơ sở xem xét đến việc kinh nghiệm và kiến thức mà tôi đã thu được thông qua các nhiệm vụ liên quan đến việc phát triển [...] trong quá trình làm việc ở Quý công ty là bí mật doanh nghiệp và bí quyết quan

trọng đối với Quý công ty.

(b) Nhận hoặc thực hiện các công việc phát triển liên quan đến [...] mà tôi đã tham gia trong quá trình làm việc tại Quý công ty và các nhiệm vụ phát triển tương tự, bất kể hình thức hợp đồng từ phía đối thủ cạnh tranh của Quý công ty.

(*2) 競業禁止義務を課すときには補償手当を支給する場合には、以下のような定めを設ける例も考えられる。

第○条 (補償手当)

私は、本誓約書の遵守のため、貴社給与及び退職金のほか、補償手当○○○ベトナムドンの交付を受けたことを確認いたします。

Điều ○. Trợ cấp bồi thường

Tôi xác nhận rằng để đổi lấy việc tuân thủ cam kết này, ngoài tiền lương và tiền thôi việc, tôi đã nhận được khoản trợ cấp bồi thường là [...] Đồng.

(*3) 秘密情報の帰属に関して、以下のような誓約事項を設ける例も考えられる。

第○条 (秘密情報の帰属)

第 1 条各号の秘密情報は貴社に帰属することを確認いたします。また当該秘密情報に関し、私に帰属する一切の権利を貴社に譲渡し、貴社に対し当該秘密情報が私に属している旨の主張を行いません。

Điều ○. Quyền sở hữu thông tin bảo mật

Tôi xác nhận rằng thông tin bảo mật trong các khoản của Điều 1 thuộc sở hữu của Quý công ty. Ngoài ra, tôi sẽ chuyển nhượng tất cả các quyền của tôi đối với các thông tin bảo mật này cho Quý công ty và sẽ không yêu cầu quyền sở hữu đối với các thông tin bảo mật này.

(*4) 秘密保持義務が存続する期間について設定するため、以下のような条項を追加する例も考えられる。

第○条 (期間、終了)

本誓約書の有効期間は、○○年間とします。ただし、第1条各号の秘密情報が公知となった場合は、その時点をもって本誓約書は終了することとします。

Điều 0. Thời hạn, chấm dứt

Cam kết này có hiệu lực trong [...] năm. Tuy nhiên, trong trường hợp thông tin bảo mật tại các khoản của Điều 1 được công khai, cam kết này sẽ bị chấm dứt tại thời điểm đó.

4. 取引先との秘密保持契約書の例

<日本語>

秘密保持契約書 (*1)

●● (以下「甲」という。) と×× (以下「乙」という。) とは、_____について検討するにあたり (以下「本取引」という。)、甲又は乙が相手方に開示する秘密情報の取扱いについて、以下のとおりの秘密保持契約 (以下「本契約」という。) を締結する。

第1条 (秘密情報) (*2) (*3) (*4)

本契約における「秘密情報」とは、甲又は乙が相手方に開示し、かつ開示の際に秘密である旨を明示した技術上又は営業上の情報、本契約の存在及び内容その他一切の情報をいう。

ただし、開示を受けた当事者が書面によってその根拠を立証できる場合に限り、以下の情報は秘密情報の対象外とするものとする。

- (a) 開示を受けたときに既に保有していた情報
- (b) 開示を受けた後、秘密保持義務を負うことなく第三者から正当に入手した情報
- (c) 開示を受けた後、相手方から開示を受けた情報に関係なく独自に取得し、又は創出した情報
- (d) 開示を受けたときに既に公知であった情報
- (e) 開示を受けた後、自己の責めに帰し得ない事由により公知となった情報

第2条 (秘密情報等の取扱い)

1. 甲又は乙は、相手方から開示を受けた秘密情報及び秘密情報を含む記録媒体若しくは物件 (複写物及び複製物を含む。以下「秘密情報等」という。) の取扱いについて、次の各号に定める事項を遵守するものとする。
 - (a) 情報取扱管理者を定め、相手方から開示された秘密情報等を、善良なる管理者としての注意義務をもって厳重に保管、管理する。
 - (b) 秘密情報等は、本取引の目的以外には使用しないものとする。
 - (c) 秘密情報等を複製する場合には、本取引の目的の範囲内に限って行うものとし、その複製物は、原本と同等の保管、管理をする。 (*5)
 - (d) 秘密情報等の漏えい、紛失、盗難、盗用等の事態が発生し、又はその

おそれがあることを知った場合は、直ちにその旨を相手方に書面をもって通知する。

(e) 秘密情報の管理について、取扱責任者を定め、書面をもって取扱責任者の氏名及び連絡先を相手方に通知する。 (*6)

2. 甲又は乙は、次項に定める場合を除き、秘密情報等を第三者に開示する場合には、書面により相手方の事前承諾を得なければならない。この場合、甲又は乙は、当該第三者との間で本契約書と同等の義務を負わせ、これを遵守させる義務を負うものとする。
3. 甲又は乙は、法令に基づき秘密情報等の開示が義務づけられた場合には、事前に相手方に通知し、開示につき可能な限り相手方の指示に従うものとする。

第3条（返還義務等）

1. 本契約に基づき相手方から開示を受けた秘密情報を含む記録媒体、物件及びその複製物（以下「記録媒体等」という。）は、不要となった場合又は相手方の請求がある場合には、直ちに相手方に返還するものとする。
2. 前項に定める場合において、秘密情報が自己の記録媒体等に含まれているときは、当該秘密情報を消去するとともに、消去した旨（自己の記録媒体等に秘密情報が含まれていないときは、その旨）を相手方に書面にて報告するものとする。

第4条（損害賠償等）

甲若しくは乙、甲若しくは乙の従業員若しくは元従業員又は第2条第2項の第三者が相手方の秘密情報等を開示するなど本契約の条項に違反した場合には、甲又は乙は、相手方が必要と認める措置を直ちに講ずるとともに、相手方に生じた損害を賠償しなければならない。

第5条（有効期限）

本契約の有効期限は、本契約の締結日から起算し、満〇年間とする。期間満了後の〇か月前までに甲又は乙のいずれからも相手方に対する書面の通知がなければ、本契約は同一条件でさらに〇年間継続するものとし、以後も同様とする。

第6条（協議事項）

本契約に定めのない事項について又は本契約に疑義が生じた場合は、協議の上解決する。

第7条（準拠法・管轄）（*7）（*8）

1. 本契約は、ベトナム法に準拠し、ベトナム法に従って解釈される。
2. 本契約から又はそれに関連して本契約の当事者間に生ずるすべての紛争は、Vietnam International Arbitration Centre (VIAC)において、同センターの仲裁規則に基づく仲裁により、終局的に解決される。仲裁地は[国又は都市]とする。仲裁手続において使用される言語は、[言語名]とする。

本契約成立の証として本書2通を作成し、甲乙署名押印のうえ、各1通を保有する。（*9）（*10）

年 月 日

（甲）

（乙）

<ベトナム語>

THỎA THUẬN BẢO MẬT

●● (sau đây gọi là "Bên A") và ●● (sau đây gọi là "Bên B") ký kết thỏa thuận bảo mật (dưới đây gọi là "Thỏa Thuận") về việc xử lý thông tin bảo mật do Bên A hoặc Bên B tiết lộ cho Bên kia trong quá trình tìm hiểu về _____ (dưới đây gọi là "Giao Dịch") như sau.

Điều 1. Thông tin bảo mật

Trong Thỏa Thuận, "thông tin bảo mật" có nghĩa là thông tin kỹ thuật hoặc kinh doanh được chỉ rõ là thông tin bảo mật mà Bên A hoặc Bên B tiết lộ cho Bên kia, và sự tồn tại, nội dung và tất cả các thông tin khác của Thỏa Thuận.

Tuy nhiên, các thông tin dưới đây sẽ không được xem thông tin bảo mật nếu Bên nhận tiết lộ có bằng chứng có thể chứng minh điều đó bằng văn bản.

(a) Thông tin đã có tại thời điểm nhận tiết lộ

(b) Thông tin thu được một cách hợp pháp từ bên thứ ba không có nghĩa vụ bảo mật sau khi nhận tiết lộ

- (c) Thông tin thu được hoặc được tạo ra một cách độc lập sau khi nhận được tiết lộ mà không liên quan đến thông tin được Bên kia tiết lộ
- (d) Thông tin đã được biết đến rộng rãi khi nhận được tiết lộ
- (e) Thông tin được biết đến rộng rãi sau khi nhận được tiết lộ bởi các lý do không thuộc về lỗi của Bên nhận được tiết lộ

Điều 2. Xử lý thông tin bảo mật

1. Bên A và Bên B sẽ tuân thủ các nội dung dưới đây về việc xử lý thông tin bảo mật cũng như phương tiện ghi âm hoặc tài sản có chứa thông tin bảo mật (bao gồm cả bản chụp và bản sao, sau đây được gọi chung là "Thông Tin Bảo Mật") nhận được từ Bên kia.

(a) Chỉ định người quản lý xử lý thông tin, và tiến hành lưu trữ và quản lý nghiêm ngặt với nghĩa vụ cẩn trọng của người quản lý đối với Thông Tin Bảo Mật do Bên kia tiết lộ.

(b) Thông Tin Bảo Mật sẽ không được sử dụng cho bất kỳ mục đích nào khác ngoài mục đích của Giao Dịch.

(c) Việc sao chép Thông Tin Bảo Mật sẽ chỉ được thực hiện trong phạm vi mục đích của Giao Dịch và các bản sao sẽ được lưu giữ và quản lý tương tự như bản gốc.

(d) Ngay lập tức thông báo bằng văn bản cho Bên kia khi biết về việc xảy ra hoặc việc có khả năng xảy ra rò rỉ, mất mát, đánh cắp.

(e) Chỉ định người chịu trách nhiệm xử lý quản lý thông tin bảo mật và thông báo bằng văn bản cho Bên kia về họ tên và thông tin liên lạc của người chịu trách nhiệm xử lý.

2. Phải được sự đồng ý trước của Bên kia bằng văn bản khi tiết lộ Thông Tin Bảo Mật cho bên thứ ba, ngoại trừ trường hợp được quy định tại Khoản 3 dưới đây. Trong trường hợp này, Bên A hoặc Bên B sẽ có nghĩa vụ ràng buộc đối với bên thứ ba các nghĩa vụ tương tự như nghĩa vụ trong Thỏa Thuận và buộc bên thứ ba phải tuân thủ nó.

3. Trường hợp Bên A hoặc Bên B có nghĩa vụ tiết lộ Thông Tin Bảo Mật theo quy định của pháp luật thì phải thông báo trước cho Bên kia, và trong khả năng có thể phải làm theo hướng dẫn của Bên kia về việc tiết lộ thông tin.

Điều 3. Nghĩa vụ hoàn trả

1. Phương tiện ghi, tài sản và bản sao của chúng (sau đây gọi là "Phương Tiện Ghi") chứa Thông Tin Bảo Mật do Bên kia tiết lộ theo Thỏa Thuận sẽ được trả lại ngay lập tức cho Bên kia trong trường hợp không còn cần thiết hoặc khi có yêu cầu của Bên kia.

2. Trong trường hợp quy định tại Khoản trên, nếu Thông Tin Bảo Mật được đưa vào Phương Tiện Ghi cá nhân thì phải xóa Thông Tin Bảo Mật này và báo cáo cho Bên kia

bằng văn bản về việc đã xóa (hoặc báo cáo về việc Thông Tin Bảo Mật không được đưa vào Phương Tiện Ghi cá nhân).

Điều 4. Bồi thường thiệt hại

Trường hợp Bên A hoặc Bên B, nhân viên hoặc cựu nhân viên của Bên A hoặc Bên B, hoặc bên thứ ba tại Khoản 2 Điều 2 vi phạm các quy định của Thỏa Thuận, chẳng hạn như tiết lộ Thông Tin Bảo Mật của Bên kia, thì Bên A hoặc Bên B sẽ phải ngay lập tức tiến hành các biện pháp mà Bên kia xét thấy cần thiết và cùng với đó phải bồi thường thiệt hại phát sinh cho Bên kia.

Điều 5. Thời hạn hiệu lực

Thỏa Thuận sẽ có hiệu lực tròn 00 năm tính từ ngày ký kết. Trừ khi Bên A hoặc Bên B thông báo bằng văn bản cho Bên kia trước 00 tháng trước khi hết thời hạn hiệu lực, Thỏa Thuận sẽ tiếp tục trong 00 năm nữa với cùng điều kiện. Quy định này cũng sẽ được áp dụng tương tự cho những lần gia hạn tiếp theo.

Điều 6. Thảo luận

Khi phát sinh bất đồng về các vấn đề không được quy định trong Thỏa Thuận hoặc về Thỏa Thuận thì các vấn đề đó sẽ được giải quyết sau khi tiến hành thảo luận.

Điều 7. Luật điều chỉnh và cơ quan giải quyết tranh chấp

1. Thỏa Thuận được điều chỉnh và giải thích theo luật Việt Nam.
2. Tất cả các tranh chấp phát sinh từ hoặc liên quan đến Thỏa Thuận giữa các Bên của Thỏa Thuận sẽ được giải quyết bằng hình thức trọng tài theo quy tắc trọng tài của Trung tâm Trọng tài Quốc tế Việt Nam (VIAC). Địa điểm trọng tài sẽ là *[quốc gia hoặc thành phố]*. Ngôn ngữ được sử dụng trong quá trình tố tụng trọng tài sẽ là *[tên ngôn ngữ]*.

ĐỂ LÀM BẰNG, Thỏa Thuận được lập thành 2 bản, Bên A và Bên B mỗi Bên giữ một bản sau khi ký tên và đóng dấu.

Ngày.....Tháng.....Năm.....

Bên A:

Bên B:

※本参考書式は、ハンドブック参考資料2の第4（P.163～164）をベースにしつつ、ベトナムの法令及び慣行に基づき、一部内容を修正し、注を加えたものである。

(*1) 秘密保持契約書を締結する場合のほか、業務提携に係る契約の中で上記の例のような秘密保持条項を盛り込む場合も考えられる。なお、本例のように、業務提携に係る契約とは別に秘密保持契約を締結する場合には、業務提携に係る契約書において、別途、秘密保持契約書を締結する旨を明示し、何に関連する秘密保持契約であるのか等、契約関係を明確にすることが有効である。

(*2) この他、業務提携に向けた検討の事実それ自体が秘密情報に含まれると定めることもある。その場合、業務提携の検討の事実については、第5条に定める有効期限は他の秘密情報と比べて相対的に短く、自動更新条項は置かずに6か月～2年程度となることが一般的である。また、業務提携を合意した時点での当該業務提携の事実についての公表は、事前に双方同意のもとで行う旨を併せて規定することも考えられる。

(*3) 秘密保持の対象とする情報の定義と呼称（例えば、「企業秘密」、「秘密情報」など。）については、当該開示の趣旨や取引慣行等に応じて様々なものが考えられる。なお、上記では「一切の情報」と書いているが、秘密保持の対象となる情報の特定ができる場合には、できる限り具体的に行うことが重要である。

(*4) 秘密情報の対象をより明確化するためには、秘密保持の対象情報を別紙でリスト化し、随時更新することも考えられ、その場合には以下の規定を追加することも考えられる。

甲が乙に秘密である旨を指定して開示する情報は、別紙のとおりである。なお、別紙は甲と乙とが協力し、常に最新の状態を保つべく適切に更新するものとする。

Thông tin mà Bên A chỉ định là bí mật và tiết lộ cho Bên B sẽ như phụ lục đính kèm. Bên A và Bên B sẽ hợp tác để phụ lục đính kèm luôn ở trong tình trạng mới và được cập nhật một cách thích hợp.

また、口頭や映像等で情報が開示される場合に備え、以下の規定を追加すること

も考えられる。

甲又は乙が口頭により相手方から開示を受けた情報については、改めて相手方から当該事項について記載した書面の交付を受けた場合に限り、相手方に対し本規定に定める義務を負うものとする。

Bên A hoặc Bên B sẽ có nghĩa vụ quy định tại Điều này với Bên kia đối với thông tin mà Bên A hoặc Bên B nhận được thông qua việc tiết lộ bằng miệng từ Bên kia, ngoại trừ trường hợp nhận được từ Bên kia tài liệu bằng văn bản ghi lại nội dung đó.

口頭、映像その他その性質上秘密である旨の表示が困難な形態又は媒体により開示、提供された情報については、開示者が相手方に対し、秘密である旨を開示時に伝達し、かつ、当該開示後〇日以内に当該秘密情報を記載した書面を秘密である旨の表示をして交付することにより、秘密情報とみなされるものとする。

Các thông tin được tiết lộ hoặc cung cấp bằng miệng, video hoặc bằng các hình thức khác mà dựa trên bản chất của nó khó để xác định được là bí mật, hoặc bằng các phương tiện khác, sẽ được xem là thông tin bảo mật thông qua việc Bên tiết lộ thông báo cho Bên kia rằng thông tin đó là bí mật tại thời điểm tiết lộ và gửi văn bản chứa thông tin bảo mật đó trong đó chỉ ra rằng đó là thông tin bảo mật trong vòng [...] ngày sau khi tiết lộ.

- (*5) 複製を行うことについては、事前の書面による承諾を求めると、受領者において情報の円滑な活用が阻害される可能性が懸念される。そこで、以下のような条項を設け、いつどのような複製物を作成したかをリスト化し、返還・消去の対象を明確化することも考えられる。

複製物を作成した場合には、複製の時期、複製された記録媒体又は物件の名称を別紙のとおり記録し、相手方の求めに応じて、当該記録を開示する。

Khi tạo lập một bản sao, các Bên sẽ ghi lại thời gian sao chép, tên của phương tiện ghi âm hoặc tài sản được sao chép trong tờ đính kèm và bản ghi này sẽ được tiết lộ theo yêu cầu của Bên kia.

- (*6) 取扱責任者等、秘密情報の授受を行う窓口を決定し、当該窓口経由でのみ秘密情報の開示を行う場合も考えられる。

- (*7) ベトナムの民法においては、当該契約に外国の要素が含まれている場合にのみ、外国法を選択することを認めている（民法第 663 条、第 683 条 1 項）。ここでいう外国の要素とは、契約当事者に外国企業が含まれる場合、権利関係

の成立・履行・消滅がすべて国外で生じている場合、又は国外の資産を対象とした契約であるといった場合に認められる。日本企業のベトナム子会社はベトナム法人として扱われるため、かかる子会社がベトナム企業と契約する場合には、ベトナム法人同士の契約ということになるので、原則として外国の要素があるものとは認められない。したがって、外国資本の企業を含むベトナム企業間の契約で、その締結や履行の一部でもベトナム国内で行われるものは、多くの場合ベトナム法を準拠法としなければならない。

(*8) ベトナム企業が当事者に含まれる契約上の紛争解決方法としては、ベトナムの裁判、ベトナム国内の仲裁、ベトナム国外の仲裁の 3 つが現実的な選択肢として考えられる。また、付随的にベトナム国内の調停を利用することも考えられる。なお、日本の裁判を紛争解決の方法とすることは、ベトナム企業側が日本の裁判所を管轄裁判所とすることに合意することは期待しにくいこと、日本とベトナムの間で判決の承認及び執行に関する条約が締結されておらず、日本の裁判所による判決の承認・執行をベトナム国内で行うことは非常に困難であることなどから、現実的な選択肢ではないと考えられる。

ベトナム国内の仲裁における仲裁判断は、ベトナム裁判所の判決と同様に執行が可能である。以前はベトナムの国内仲裁制度には制度上の制約があることが指摘されていたが、2011 年 1 月に新商事仲裁法が施行されたことにより、ベトナムの国内仲裁における不備がある程度解消され、ベトナムにおける仲裁を紛争解決方法の選択肢の一つとして検討する余地が出てきた。実際、ベトナムの国内仲裁機関の中でも国際仲裁に関して最も権威があると評価されている Vietnam International Arbitration Centre (VIAC) における仲裁の件数は近年増加している。

そこで、本書式では、VIAC を仲裁機関として使用する場合は条項例を記載している。

ただし、国内仲裁に対しては、国内の裁判所による一定の関与が認められており、仲裁権限が否定されたり、形式的な手続上の瑕疵を理由に仲裁判断を取り消されたりするケースも出てきているため、その信頼性については留意が必要である。

なお、VIAC の推奨する仲裁合意条項は以下である²⁶。

===

“Any dispute arising out of or in relation with this contract shall be resolved by arbitration at the Vietnam International Arbitration Centre (VIAC) in accordance with its

²⁶ <https://www.viac.vn/en/model-clause.html> [最終アクセス日：2020 年 11 月 18 日]

Rules of Arbitration”.

“Any dispute arising out of or in relation with this contract shall be resolved by arbitration at the Vietnam International Arbitration Centre at the Vietnam Chamber of Commerce and Industry (VIAC) in accordance with its Rules of Arbitration”.

Parties may wish to consider adding:

(a) the place of arbitration shall be [city and/or country].

*(b) the governing law of the contract [is/shall be] the substantive law of [].**

*(c) the language to be used in the arbitral proceedings shall be [].***

Note:

** For disputes which involve a foreign element.*

*** For disputes which involve a foreign element or disputes in which at least one party is an enterprise with foreign investment capital.*

===

(*9) 実際に秘密保持契約書を締結する場面では、日本語とベトナム語、英語とベトナム語など契約書を複数の言語で作成する場合も少なくないと思われる。それらの間にニュアンスの相違等が生じることは避けがたいため、いずれの言語が優先するかを定めておくべきである。例えば、以下の規定を追加することが考えられる。

第〇条（言語）

本契約の言語は、日本語とする。本契約に参考のためにベトナム語による翻訳文が作成される場合においても、日本語版のみが契約として効力を有し、ベトナム語訳にはかかる効力がない。

Điều 〇. Ngôn ngữ

Ngôn ngữ của Thỏa Thuận là tiếng Nhật. Kể cả trong trường hợp bản dịch tiếng Việt được soạn thảo cho mục đích tham khảo cho Thỏa Thuận thì chỉ có bản tiếng Nhật có hiệu lực như một bản thỏa thuận, bản dịch tiếng Việt sẽ không có hiệu lực này.

(*10) 従来ベトナムでは企業の社印を計画投資局に通知する必要があったが、2021年1月に施行された新企業法において、企業はその印章として社印又は電子署名を決定し、社内の規則に従って保存するものとして、当該通知は不要となった。もっとも、商慣習上、ベトナム国内の契約書締結時には、代表者の

署名に加えて社印の押印（割印も含む）を求められることが多い。

※ Quý khách đến tham quan, họp và tiến hành kinh doanh tại công ty chúng tôi xin vui lòng điền các thông tin dưới đây khi vào công ty.
※ Trên quan điểm bảo mật thông tin của công ty, quý khách vui lòng đồng ý với nội dung ghi trên phiếu bảo đảm bên phải và đánh dấu xác nhận vào ô "Đồng ý với nội dung bảo đảm ở trên" tại bảng dưới đây.
※ Xin quý khách lưu ý rằng nếu không đồng ý với nội dung của phiếu bảo đảm được ghi ở bên phải, công ty chúng tôi có thể từ chối quý khách vào công ty.

Công ty ●●

※ 当社に見学、面会、商談にお越しのお客様は、当社にお入りになる際、以下のご記入をお願い致します。
※ 当社の情報の秘密保持の観点から、右の保証書の内容をご了承の上、下表の「上記保証書に同意」の欄にチェックのご記入をお願い致します。
※ 右の保証書に同意頂けない場合、当社は、お客様の立ち入りをお断りする場合がございますことをご了承承願します。

●●会社

NO	日付 Ngày	会社名 Tên công ty	氏名 Họ và tên	目的 Mục đích	入場時間 Giờ vào	退場時間 Giờ ra	上記保証書に同意 Bên ý với giấy bảo đảm ở trên	撮影許可 Được phép chụp ảnh (Có/Không)	責任者署名 Chữ ký người chịu trách nhiệm
1	2020●●	●●	●●	●●	10:00	15:00	✓	有無	●●
2					:	:		有無	
3					:	:		有無	
4					:	:		有無	
5					:	:		有無	

Phiếu bảo đảm

Kính gửi công ty ●●
Tôi bảo đảm sẽ tuân thủ các vấn đề dưới đây khi tham quan, họp và tiến hành kinh doanh tại Quý công ty.

Điều 1. Bảo mật
Tôi sẽ tuân thủ các điều sau đây:

- (1) Không chụp ảnh, ghi âm, quay phim trong nhà máy hoặc văn phòng khi chưa được sự đồng ý từ người phụ trách của Quý công ty.
(2) Không lan truyền thông tin bí mật được trong nhà máy hoặc văn phòng của Quý công ty ra bên ngoài mà không có sự đồng ý trước bằng văn bản của Quý công ty.

Điều 2. Bồi thường thiệt hại
Trường hợp vi phạm các quy định trên gây ra thiệt hại cho Quý công ty, tôi đồng ý chịu mọi trách nhiệm, và cùng với công ty chủ quản chịu trách nhiệm bồi thường thiệt hại cho Quý công ty theo quy định của pháp luật có liên quan.

保証書

●●会社殿
貴社の見学、面会、商談においては、以下の事項を遵守することを保証致します。

第1条 (秘密保持)

- 以下の事項を遵守致します。
① 貴社担当者の同意なく、工場内またはオフィス内で写真撮影、録音、動画撮影を行いません。
② 貴社の事前の書面による同意なく、貴社工場またはオフィス内で知得した情報を外部に伝達しません。

第2条 (損害賠償)
上記規定に違反し、貴社が損失を蒙った場合には、一切の責任を負うこと、及び、所属会社とともに、関連法令の規定に従い、貴社に対して、損害責任を負担することに同意致します。

(*1) 本書式のように、入館記録への署名と、誓約書とを一体化することで、署名を要請しやすくなると考えられる。

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。

[調査受託]

長島・大野・常松法律事務所ハノイ・オフィス

独立行政法人 日本貿易振興機構 ハノイ事務所

2021 年 3 月

禁無断転載

本報告書の作成においては、できるだけ正確な情報の提供を心がけておりますが、本報告書で提供している情報は、調査時点で入手・判明し得たものであり、ご利用に際してはこの点をご留意の上、ご活用ください。