経済産業省委託

令和５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））報告書

2024 年 3 月

独立行政法人　日本貿易振興機構
知的資産部

目次

［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。令和２年度の「企業における営業秘密管理に関する実態調査」[1]では、９割以上の企業が「営業秘密の漏えいに関して脅威に感じているものがある」と回答しており、その中では「海外の拠点・取引先・連携先を通じた自社秘密情報の漏えいについて対策が必要と考えている」との声も聞かれ、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。営業秘密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、営業秘密管理の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、管理体制の確立・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、現地事情に精通した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。

[1]令和３年３月、独立行政法人情報処理推進機構（ＩＰＡ）が公表
（https://www.ipa.go.jp/archive/files/000089191.pdf）。同調査報告書 31 頁を参照。

［２］個別支援

１．概観

中国に進出する日系企業は、31,000 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（令和２年）[2]によれば、日系企業の拠点数上位 10 ヶ国中５ヶ国をＡＳＥＡＮが占めている。また、令和４年８月～９月にかけてＪＥＴＲＯが実施した調査によれば、事業拡大先の 1 位にインド、２位ベトナム、５位メキシコ、６位オランダ、10 位インドネシア、11 位ドイツ、13 位フランス、14 位タイ、15 位英国、16 位中国があげられていたことから、中国、ベトナム、インドネシア、タイに加え、インド、欧州一部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日本企業や現地日系企業等（中国８社、タイ 1 社、インドネシア 3 社、ドイツ 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	北京市（進出予定）	2023 年 8 月 15 日～2024 年 1 月 11 日
2	B 社	遼寧省	2023 年 9 月 19 日～2024 年 1 月 15 日
3	C 社	山東省	2023 年 9 月 4 日～2024 年 1 月 11 日
4	D 社	上海市	2023 年 9 月 28 日～2023 年 12 月 11 日
5	E 社	江蘇省	2023 年 9 月 19 日～2024 年 1 月 26 日
6	F 社	浙江省	2024 年 1 月 4 日～2024 年 1 月 30 日
7	G 社	上海市	2023 年 12 月 13 日～2024 年 1 月 31 日
8	H 社	江蘇省	2024 年 1 月 10 日～2024 年 1 月 30 日

（２）タイ

	企業	支援先拠点	支援期間
1	I 社	バンコク	2023 年 12 月 12 日～2024 年 1 月 31 日

[2] 令和 2 年外務省が公表（https://www.mofa.go.jp/mofaj/ecm/ec/page22_003410.html?msclkid=3137ebb4ab4e11ecb704a268e6c3bc4f）。

（3）ベトナム

	企業	支援先拠点	支援期間
1	J 社	ホーチミン市	2023 年 8 月 31 日～2024 年 1 月 26 日
2	K 社	ホーチミン市	2023 年 9 月 6 日～2024 年 1 月 30 日
3	L 社	2024 年度に進出予定	2024 年 12 月 26 日～2024 年 1 月 29 日

（4）インドネシア

	企業	支援先拠点	支援期間
1	M 社	ジャカルタ首都特別州	2023 年 9 月 5 日～2024 年 1 月 23 日
2	N 社	ジャワバラット州	2023 年 10 月 13 日～2024 年 1 月 29 日
3	O 社	ジャカルタ首都特別州	2023 年 10 月 19 日～2024 年 1 月 30 日

（5）インド

応募実績なし

（6）欧州一部

	企業	支援先拠点	支援期間
1	P 社	ヘッセン州（フランクフルト）	2023 年 12 月 4 日～2024 年 1 月 30 日

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 16 社中、11 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	F 社	秘密保持規定の起草、従業員との秘密保持誓約書の改定。
2	B 社	秘密管理の見直し。委託契約書(機密関連部分)が開設された。
3	G 社	秘密保持契約書。
4	J 社	秘密保持契約書。
5	P 社	リバースエンジニアリング禁止事項が対顧客への NDA へ追記された。
6	A 社	社内における営業秘密漏洩の研修のミーティング。
7	C 社	PC ロックまでの時間設定、現場貼付け資料の機密マーク表示など。
8	O 社	営業秘密漏洩に関する内部規定の設定を予定している。
9	K 社	書類内容の見直し。
10	M 社	サポートの元、新たに更新する予定の、社内機密データ取り扱いに関するポリシーの適用。
11	E 社	来社時の訪問カード。

アンケート回答企業 16 社中、7 社で営業秘密漏えい防止策の導入の検討を始めた対策。

	企業	導入の検討を始めた対策
1	H 社	レビューして頂いた規程類の見直しの検討を始めている。
2	F 社	入出門時の署名、入門バッチの採用。
3	P 社	入社時に署名する書類内の秘密漏洩についての条項にて、専門家のアドバイスに沿って情報の定義や従業員の責務の明確化。
4	A 社	中国ビジネスでの秘密保持契約の再作成（今までの契約では不十分だったため)。
5	C 社	外来者訪問時の機密情報保持契約書の締結及び現場訪問ルートの事前確定、重要職場のポジション職責説明書の締結など。
6	K 社	社内手続きの見直し。
7	E 社	ファイルの管理や整理、重要性のランク付け。

［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。

２．個別支援企業募集セミナー

各国の専門家より営業秘密漏えい対策について講演を行い、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 セミナー等を日本国内（東京）及び中国（上海、青島、広州）で開催した。

（１） 日本

・ 実施日時　2023 年 8 月 9 日（水）15：00～17：20　インド、ベトナム
　開催形式　WEB セミナー
　参加人数　227 名

・ 実施日時　2023 年 9 月 28 日（金）16：00～17：35　南アフリカ共和国
　開催形式　WEB セミナー
　参加者数　55 名

（２） 中国

・ 実施日時　2023 年 8 月 25 日（金）14：00～16：30　上海
　開催形式　対面＋WEB セミナー
　参加人数　対面 40 名、WEB セミナー141 名　計 181 名

・ 実施日時　2023 年 9 月 14 日（木）16：00～17：30　青島
　開催形式　対面
　参加人数　42 名

・ 実施日時　2023 年 11 月 7 日（火）14：30～16：00　広州
　開催形式　WEB セミナー
　参加人数　36 名

３．成果普及セミナー

メキシコの専門家より、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　2024年1月19日（金）9：00～10：20
　　開催形式　WEBセミナー
　　参加人数　163名

４．その他

官民の実務者間において、営業秘密の漏えいに関する最新手口やその対策に係る情報交換を行う場として、2023年6月28日に開催された「営業秘密官民フォーラム」において、海外における営業秘密管理及び本事業の取組について紹介した。

［４］マニュアル・調査レポート作成

１．概観

メキシコ及び中国、インドについて、関係法令における営業秘密の定義・対象範囲（侵害行為）・法的措置（民事救済・刑事罰等）、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）からなる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

メキシコにおける営業秘密管理マニュアル

2024 年 3 月

独立行政法人　日本貿易振興機構

メキシコ事務所

目次

はじめに

現代社会においては、情報技術の発達や多様な情報関連サービスの充実により、事業活動に関連し、創出、収集される情報も劇的に増加し、また、世界各地に点在する拠点において、瞬時に情報を共有、連携できる環境が整っている。その一方で、企業の情報が漏えい、盗用されるリスクも高まっていると考えられる。技術やノウハウ、取引先や顧客の情報などは企業にとって大切な財産であり、これにより、企業の競争力が促進される。一方、一旦その情報が漏えいしてしまうと、営業機会の損失に繋がり大きな損害となってしまう。

情報漏えいはどのように発生するのか。その原因は様々であろうが、その保護体制・システムが最も弱いところから漏えいするのである。国内外を問わず、複数拠点で事業を展開する企業においては、もちろん、その情報取扱に応じて差はあるのだが、全ての拠点で同等の情報保護体制・システムを敷くことが求められる。日系企業においては、日本の本社・支店においては、十分な情報保護対策が採られている一方で、その海外拠点では、十分な対策がとられていないこともあるようである。企業の情報を保護するためには、人材や資金が乏しい海外拠点でこそ、情報保護対策を強化する必要があるのではなかろうか。

メキシコにも多くの日系企業が海外拠点を設けているが、製造・営業分野に注力し、管理部門、特に情報保護といった分野に対しては、対策が十分でない企業も多いようである。

なお、残念ながらメキシコの情報リテラシーは高くないと感じている。離職率も高く、こういった点からも情報漏えいリスクが高いと危惧している。日本とメキシコでは、法制度の違いはあるが、営業秘密に対する基本的な考え方や対策は大きく変わらない。もちろん、言語の違い、文化・慣習の違いが大きくあることから、一定の「応用」が必要になるのだが、日本の情報管理体制や保護対策をメキシコに応用させる方法が、効率的で効果的な方法でないかと考える。

本マニュアルは、2 部構成となっており、1 部では法制度を、2 部では漏えい対策を取り上げた。特に 2 部では、メキシコ特有の対策といったものはなく、日本のそれと共通するものであることから、日本で情報保護対策を担当する方にとってはなじみのある内容となっていることであろう。

メキシコで事業を営む日系企業の営業秘密保護のために本マニュアルを少しでも役立てていただければ幸いである。

第Ⅰ部. 法制度

（1）メキシコにおける営業秘密の定義

日本でいう「営業秘密」に近い概念として、メキシコでは連邦産業財産権保護法（Ley Federal de Protección a la Propiedad Industrial、以下「法」という。）に規定される「Secreto Industrial」（以下、「営業秘密」という。）が挙げられる。

営業秘密の定義は、法163条1号に、次のように定義される。

営業秘密：法的管理を行う者が秘密を保持する産業用及び商業用のすべての情報。この情報は経済活動を行う上で第三者に対する競争上若しくは経済上の優位性を獲得又は維持するもので，その秘密性が維持され，アクセスを制限する十分な手段とシステムとを採用されていること。
営業秘密の情報は，書類，電子，磁気媒体，光ディスク，マイクロフィルム，フィルム又は他の既知の情報媒体で表示される。
以下に示される公知公用の情報は営業秘密とはみなされない；通常に使用される分野の人々に一般的に知られている若しくは簡単にアクセスできる情報又は法律の規定若しくは裁判所の命令によって開示されなければならない情報。
営業秘密を法的に管理する者によって官庁に提出される情報は，それが法律の規定により開示される，免許，許可，認可，登録，その他官庁の如何なる措置取得のために提出される場合も，公知公用の情報とみなされない[vi]*。*

すなわち、情報が営業秘密とみなされる条件が次のとおり導かれる。

i)産業的・商業的価値があること
ii)機密性が維持されていること
iii)情報に対し機密に保つための合理的措置が施されていること

日本において営業秘密に求められる要件 i)有用性、ii）秘密管理性、iii）非公知性に非常によく似ている。

日本での営業秘密は、不正競争防止法に規定されており、その2条6項において、「この法律において「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又は営業上の秘密であって、公然と知られていないものをいう。」と定義されており、前述の3つの要件の詳細は次のとおりである。

i)有用性：当該情報が客観的にみて、事業活動に有用であること
ii)秘密管理性：企業が当該情報を秘密裏に管理しようとする意思が、何らかの措置によって従業員や取引先に対して明確に示されており、かつ、当該意思について従業員等が認識できるような状態にあること
iii)非公知性： 当該情報が、一般的には知られておらず、又は容易に知ることができないこと

従って、営業秘密の要件は非常によく似ているといえ、次のようにまとめることができる。

【営業秘密の要件】

要件	メキシコ	日本
	産業財産権保護法 136 条 1 号	不正競争防止法 2 条 6 項
有用性	産業的・商業的価値があること	当該情報が客観的にみて、事業活動に有用であること
秘密管理性	機密性が維持されていること	企業が当該情報を秘密裏に管理しようとする意思が、何らかの措置によって従業員や取引先に対して明確に示されており、かつ、当該意思について従業員等が認識できるような状態にあること
非公知性	情報に対し機密に保つための合理的措置が施されていること	当該情報が、一般的には知られておらず、又は容易に知ることができないこと

なお、これは、メキシコが日本も加盟する TRIPS 協定（知的所有権の貿易関連の側面に関する協定）に加盟していることが挙げられる。TRIPS 協定第 39 条「開示されていない情報の保護」において、保護の対象となる情報として、「(a)当該情報が一体として又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又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」[ii]とされており、加盟国はこのような規定に基づき国内法を整備する必要があることから、このように似かよった要件となっていると考えられる。

しかしながら、メキシコにおいては、これらの各要件について、どのような場合を指すかといった具体的な指針などは示されていない。

法 163 条は営業秘密に該当しない情報を「通常に使用される分野の人々に一般的に知られている若しくは簡単にアクセスできる情報又は法律の規定若しくは裁判所の命令によって開示されなければならない情報。営業秘密を法的に管理する者によって官庁に提出される情報は，それが法律の規定により開示される，免許，許可，認可，登録，その他官庁の如何なる措置取得のために提出される場合も，公知公用の情報とみなされない」と定義することから、非公知性については、一般に知られておらず、または簡単に知ることができない情報と考えられる。

また、法 165 条、166 条は次のとおり規定する。

165 条　営業秘密を保有する者は，第三者に対して当該秘密情報を移転し又は使用を許諾することができる。使用を許諾された者は，如何なる手段かを問わず当該秘密情報を他の者に開示してはならない。

専門知識，技術援助及び基本的又は詳細エンジニアリングを提供する契約は提供される役務を構成するべき営業秘密を保護する守秘条項を含むものとし，かつ当該条項は秘密として扱われるべき要素を特定しなければならない。

166 条　職種，雇用内容，業務若しくは地位，職業慣行又は企業関係行為に基づき，秘密情報であることを告知された営業秘密に接する者は，正当な事由があり，かつ当該秘密の所有者又はその許可された利用者の同意がある場合を除いて，その秘密を開示してはならない。

従って、機密であることの明示や、守秘義務を負うものによって機密であることが確認できることが求められると考えられる。

また、法は、営業秘密に関し、行政違反と犯罪となる行為を規定している。

【行政違反（Infracciones Administrativas)】(法 386 条)

i) *工業，商業及びサービス業において不正競争を促すため，市場で競争上の優位性を獲得するため又は良好な実務と慣習に反する行為を実施するため，法的管理を履行する者又はそのことを許可された使用者の同意を得ずに，営業秘密とみなされる情報を不正に流用すること*（14 号)。

ii) *営業秘密を使用する商品又は役務を，製造，販売，販売のための申出，輸入，輸出又は保管すること。ただし，当該活動を実施する者が，法的管理を履行する者又はそのことを許可された実施権者の同意を得ず，かつ，工業，商業及びサービス業における不正競争を暗示して良好な実務と慣習に反する仕様で営業秘密が使用されていたことを知っているか又は知るための合理的な根拠を有する場合に限る*（15 号)。

※ここでいう、営業秘密は、原文では「secreto comercial」と記されている。

【犯罪（Delitos)】(法 402 条)

i) *職務上，立場上，職業上又は取引上の関係により知り得た営業秘密を含む情報について秘密性に関して警告を受けながらも，自身若しくは第三者の経済的利益を取得する目的又は営業秘密の法的管理を履行する者若しくは許可された使用者に対して損害を生じさせる目的で，第三者に開示すること。業務上知り得た営業秘密に関し、自身あるいは第三者のために経済的利益を得る目的または営業秘密の保有者に対し損害を与える目的で、保有管理者等の同意を得ずに、営業秘密を第三者に開示すること*（3 号)。

ii) *経済的利益を取得する目的又は営業秘密の法的管理を履行する者若しくは許可された使用者に対して損害を生じさせる目的で，権利なくかつ法的管理を履行する者又は許*

可された使用者の同意なく，営業秘密を使用する又は第三者に開示するために，営業秘密を掌握すること（4 号）。

iii) *経済的利益を取得する目的又は営業秘密の法的管理を履行する者若しくは許可された使用者に対して損害を生じさせる目的で，職務上，立場上，職業上又は取引上の関係により知り得た営業秘密を含む情報であって法的管理を履行する者若しくは許可された使用者からの同意のない情報又は法的管理を履行する者若しくは許可された使用者の同意なく第三者から漏洩された情報を，使用すること。業務上知り得た営業秘密に関し、経済的利益を得る目的または保有管理者等に損害を与える目的で、その保有管理者等の同意なしにこれを使用すること*（5 号）。

iv) *損害を生じさせる目的又は自己若しくは第三者の経済的利益を取得する目的で，法的管理を履行する者又は許可された使用者の同意を得ることなく，営業秘密を流用，取得，使用又は不適切に開示すること*（6 号）。

なお、法 163 条 2 号は、不適切な流用（Apropiación indebida）を次のとおり定義し、164 条はその例外を規定する。

163 条
(2)不適切な流用：工業，商業及び役務における良好な実務と慣習に反する仕様での営業秘密の取得，使用若しくは開示であって，営業秘密が当該使用及び慣習に反する仕様で取得されたことを知っていたか又は知るための合理的な根拠を有した第三者による営業秘密の取得，使用若しくは開示を含む不正競争を暗示すること。
164 条
次のものは，不適切な流用とはみなされない。
(1)営業秘密として主張されている情報から独立した発見又は創作。
(2)営業秘密に関する秘密性の責務に従うことを条件としない限りにおける，公衆に利用可能とされたか又は情報を取得する者による適法な所有である製品若しくは対象の観察，研究，分解若しくは試験，又は
(3)秘密性の責務を伴わないこと又は情報が営業秘密であったことを知らずに適法な仕様で他の者の情報を取得すること。

したがって、不正競争を意図した営業秘密の使用や開示は行政違反となり、何らかの経済的利益を取得する目的、もしくは損害を生じさせる目的による、営業秘密の流用、取得、使用、開示などは犯罪となる。

では、日本の不正競争防止法に定める侵害類型と比較したい。まず、日本の侵害類型をまとめると次のとおりである。

【日本の侵害類型】

不正競争防止法		要約
営業秘密不正取得行為 （2 条 4 号）	窃取、詐欺、強迫その他の不正の手段により営業秘密を取得する行為（以下「営業秘密不正取得行為」という。）又は営業秘密不正取得行為により取得した営業秘密を使用し、若しくは開示する行為（秘密を保持しつつ特定の者に示すことを含む。）	不正な手段による営業秘密の取得 不正取得した営業秘密の使用・開示
不正取得後悪意転得・使用・開示行為 （2 条 5 号）	その営業秘密について営業秘密不正取得行為が介在したことを知って、若しくは重大な過失により知らないで営業秘密を取得し、又はその取得した営業秘密を使用し、若しくは開示する行為	不正取得された営業秘密の取得・使用・開示
不正取得後善意転得・悪意使用・開示行為 （2 条 6 号）	その取得した後にその営業秘密について営業秘密不正取得行為が介在したことを知って、又は重大な過失により知らないでその取得した営業秘密を使用し、又は開示する行為	情報を取得後、不正取得された営業秘密であることを知り、これを使用・開示すること
図利・加害目的使用・開示行為 （2 条 7 号）	営業秘密保有者からその営業秘密を示された場合において、不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、その営業秘密を使用し、又は開示する行為	正当に開示された情報を、不正な利益を得る目的・損害を与える目的で、使用・開示すること
不正開示情報の悪意取得・使用・開示行為 （2 条 8 号）	その営業秘密について営業秘密不正開示行為（正当に取得した営業秘密を図利・加害目的で開示する行為）であること若しくはその営業秘密について営業秘密不正開示行為が介在したことを知って、若しくは重大な過失により知らないで営業秘密を取得し、又はその取得した営業秘密を使用し、若しくは開示する行為	営業秘密不正開示行為、その行為が介在したことを知って、営業秘密を取得・使用・開示すること
不正開示情報の善意取得、悪意使用・開示行為 （2 条 9 号）	その取得した後にその営業秘密について営業秘密不正開示行為があったこと若しくはその営業秘密について営業秘密不正開示行為が介在したことを知って、又は重大な過失により知らないでその取得した営業秘密を使用し、又は開示する行為	情報を取得後、その情報について営業秘密不正開示行為があったことを知り、これを使用・開示すること
不正使用行為により生じた物の譲渡行為 （2 条 10 号）	営業秘密のうち技術上の情報を不正に使用する不正使用行為により生じた物を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、輸入し、又は電気通信回線を通じて提供す	営業秘密の不正使用行為によって生じた物を譲渡・展

	る行為（当該物を譲り受けた者（その譲り受けた時に当該物が不正使用行為により生じた物であることを知らず、かつ、知らないことにつき重大な過失がない者に限る。）が当該物を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、輸入し、又は電気通信回線を通じて提供する行為を除く。）	示・輸出・輸入・提供すること

前述のメキシコの規定を要約すると次のとおりであり、対応する日本の侵害類型を当てはめると次のようになると考えられる。

【日墨侵害類型の比較】

メキシコ		日本
産業財産権保護法	要約	不正競争防止法
386 条 14 号	不正競争・市場優位性の獲得を目的とした、営業秘密の不正流用（取得・利用・開示）	営業秘密不正取得行為（2 条 4 号） 不正取得後悪意転得・使用・開示行為（2 条 5 号） 不正取得後善意転得・悪意使用・開示行為（2 条 6 号）
386 条 15 条	営業秘密を不正利用する商品・サービスの製造・販売・輸入・輸出・保管	不正使用行為により生じた物の譲渡行為（2 条 10 号）
402 条 3 号	機密であることを知りながら、図利・加害の目的で、知り得た営業秘密を開示すること	図利・加害目的使用・開示行為（2 条 7 号）
402 条 4 号	図利・加害の目的で、営業秘密を利用・開示するために、これを取得すること	営業秘密不正取得行為（2 条 4 号）
402 条 5 号	図利・加害の目的で業務上知り得た営業秘密を含む情報を使用すること 第三者が漏えいしたそのような情報を図利・加害の目的で使用すること 図利・加害の目的で業務上知り得た営業秘密を使用すること	営業秘密不正取得行為（2 条 4 号） 不正取得後悪意転得・使用・開示行為（2 条 5 号） 不正取得後善意転得・悪意使用・開示行為（2 条 6 号） 不正開示情報の悪意取得・使用・開示行為（2 条 8 号） 不正開示情報の善意取得、悪意使用・開示行為（2 条 9 号）
402 条 6 号	図利・加害の目的で営業秘密を流用・取得・使用・開示すること	営業秘密不正取得行為（2 条 4 号）

その他、関連する法規制として次のものが挙げられる。

・連邦労働法（Ley Federal del Trabajo）

連邦労働法 134 条 13 号は、労働者の義務として「直接的または間接的に生産に関与している製品の、または業務上知ることとなった技術的、商業的、製造上の秘密、および公開すると会社に損害を与える可能性がある機密事項（asuntos administrativos reservados）を厳重に管理すること」と規定する。また、47 条 9 号は「労働者が製造上の秘密を漏えいし、または、会社に不利益をもたらす機密事項を漏えいした場合」は、使用者は責任を負うことなく、当該労働者を解雇することができると規定する。

連邦労働法においては、このような秘密情報にかかる規定は、これらの他なく、その定義などは見当たらないが、「技術的、商業的、製造上の秘密、その開示が会社に損害を与えうる機密情報」も営業秘密を構成しうると考えることができる。

・一般商事会社法（Ley General de Sociedades Mercantiles）

一般商事会社法 157 条は、株式会社（sociedad anónima）において、日本の取締役に該当する Administrador の責任として、「会社内での立場上知り得た情報や事項について、それらが非公開の場合には、司法または行政当局からの要請がある場合を除き、秘密を保持しなければならない。この秘密保持義務は、任務期間中および任務終了後最長 1 年間継続する」と規定する。従って、一般商事会社法においては、「会社の非公開の情報」も営業秘密を構成しうると考えられる。

・連邦刑法（Código Penal Federal）

連邦刑法では、機密の漏えい・開示について刑罰を規定している。210 条では、正当な事由がなく、不利益を与え、また被害を受ける恐れのある人の同意を得ずに、知りうる秘密や雇用、役職、立場上知り得た秘密や秘密の通信について、これを明らかにすることに対して刑罰が規定される。さらに、211 条は、そのような開示が専門的・技術的サービスを提供する者や公務員によって行われた場合、その秘密情報が産業上のもの（carácter industrial）である場合、はその刑罰を重く規定する。

本法において、「産業上のもの（carácter industrial)」の定義や説明はないが、営業秘密も該当すると考えられる。

サマリー

営業秘密を規定する法律

👉連邦産業財産権保護法(Ley Federal de Protección a la Propiedad Industrial)

営業秘密の定義

👉法的管理を行う者が秘密を保持する産業用及び商業用のすべての情報。この情報は経済活動を行う上で第三者に対する競争上若しくは経済上の優位性を獲得又は維持するもので、その秘密性が維持され、アクセスを制限する十分な手段とシステムとを採用されていること。

★ポイント:産業的・商業的価値があること
機密性が維持されていること
情報に対し機密に保つための合理的措置が施されていること

第三者への開示

👉専門知識，技術援助及び基本的又は詳細エンジニアリングを提供する契約は提供される役務を構成するべき営業秘密を保護する守秘条項を含むものとし，かつ当該条項は秘密として扱われるべき要素を特定しなければならない。

（２）営業秘密に関する法改正状況

法は、2020 年 7 月にその前身となる産業財産権法（Ley de la Propiedad Industrial）を全面的に改正する形で制定され、2020 年 11 月に施行された。その改正の背景には、USMCA（United States-Mexico-Canada Agreement: 米国・メキシコ・カナダ協定）への準拠が挙げられる。

営業秘密に関していえば、USMCA 第 20 章において、知的財産権が規定されており、I 節に営業秘密（Trade Secret、スペイン語では「Secretos Industriales」）の規定が設けられ、国営企業による不正流用を含め、民事、刑事による強力な営業秘密保護が謳われた。

これを受け、産業財産権法においては、営業秘密に関する違反行為は、犯罪として扱われ、法でいうところの 402 条 3 号、4 号、5 号のみが規定されていたが、法 386 条 14 号、15 号、402 条 6 号の規定が改正によって追加されたことは意義が大きい。特に、386 条 15 号に規定される、営業秘密を不正利用する商品・サービスの製造・販売・輸入・輸出・保管については、これまでそのような行為を違反行為と定める規定がなかったことを鑑みると、違反行為に対する制裁の強化が図られたと考えることができる。さらに、386 条 15 号に関連し、権利侵害にもとづく行政違反の申立てに関する手続きにおいて、当局となるメ

キシコ産業財産権庁（Instituto Mexicano de la Propiedad Industrial、以下「IMPI」）が取りうる措置について、法 344 条に、法違反となる輸出入、輸送、通関手続きの停止を命じることができる（6 号）との規定が設けられている。

また、産業財産権法のもとでは、IMPI による行政違反の宣言を受け、同法で保護されている権利侵害によって生じた損害賠償を裁判通じて請求できるのみであったが、法では 396 条において、産業財産権の所有者は、IMPI の行政違反宣言を必要とせず、裁判所を通じて、侵害の結果被った損害の賠償を請求することができることとなった。このようにメキシコにおいても民事での保護が教化された。

（３）営業秘密の流出事例

管轄当局となる IMPI に直近 5 年間に申請された営業秘密にかかる違反に関する手続申請の件数を照会したところ、2023 年 10 月 9 日付の回答により、2017 年以降に 16 件の手続が申請されていることが分かった。その詳細が閲覧できたものは、結論が出た事案の 3 件のみであった。

番号（EXPEDIENTE）	ステータス
P.C.2765/2017(Z-8)28206	却下
P.C.404/2018(M-15)4899	棄却
P.C.1649/2018(I-208)18322	棄却
P.C.705/2020(Z-1)9008	手続中
P.C.706/2020(Z-2)9009	手続中
P.C.2324/2021(I-279)25074	手続中
P.C.2327/2021(I-280)25085	手続中
P.C.2339/2021(I-282)25098	手続中
P.C.1155/2022(Z-3)14367	手続中
P.C.1251/2022(I-172)15280	手続中
P.C.2147/2022(M-182)25229	却下
P.C.318/2023(I-41)4024	手続中
P.C.669/2023(I-74)7843	手続中
P.C.1937/2023(I-250)1528	手続中
P.C.1983/2023(I-251)23701	手続中
P.C.1939/2023(I-252)23702	手続中

結論が出た 3 件の詳細は、次のとおりである。

なお、各事案に関連する書類の原本は次の URL から検索が可能。

IMPI Visor de Documentos Busquéda Rapida：https://vidoc.impi.gob.mx/BusquedaRapida

事案①

番号（EXPEDIENTE）	P.C.2765/2017(Z-8)28206
結論	却下
概要	申立人は飲食店を経営する企業である。申立人は、従業員に対し、料理のレシピは会社の財産であると伝え、レシピを守ってきた。

	申立人の元従業員が相手方に雇用されており、相手方のレストランで提供される食事が、申立人の料理と味や食感が同じであるとし、相手方は、申立人の営業秘密であるノウハウを取得するために当該従業員を雇用したと主張。産業財産権法 86 条（営業秘密を取得する目的で、当該営業秘密を保有する者に雇用されている者や雇用されていた者を雇用する者は、これにより生じた損害を賠償する責任を負う）に言及し、産業財産権法 213 条 30 号（犯罪として定めるもの以外について、本法の規定に違反する行為を、行政違反とする）に基づき、IMPI に対して行政違反の宣言を求めた。
IMPI の判断	申立人の主張は、産業財産権法 213 条に規定する行政違反に該当しないとして却下した。

事案②

番号（EXPEDIENTE）	P.C.404/2018(M-15)4899
結論	棄却
概要	申立人（法人）は、数年かけて完成させた、独自の取引モデルと信用分析モデル、証券市場内の各顧客を分類した顧客データベースからなる営業秘密の所有者である。 申立人は、その従業員と雇用契約書において、当該従業員がアクセスできる情報を開示しないことを義務付けており、また守秘義務契約書も締結していた。 当該従業員は、申立人を退職したのち、申立人と同じ事業目的を持つ競合他社に就職し、当該競合会社において、申立人のデータベースを用いて、申立人のもとで働いていた時と同じ仕事を行っている。 これは、不公正な競争を引き起こしているとして、産業財産権法 213 条 1 号（不正競争や、本法が規制する事項に関連する、産業、商業およびサービスにおける優良慣行・慣習に反する行為を行うことを行政違反とする）に該当し、産業財産権法 199 条 Bis に基づき、当該競合会社に対し商品・サービス提供の中止や営業施設の閉鎖などの措置をとることを IMPI に請求した。
相手方の主張	相手方は、申立人が主張する営業秘密を使用したことを証明する証拠は何もないと主張。 また、申立人が提出した証拠に異議を申立て、データベースが相手方の所有にないことを証明する証拠を提出した。 さらに、営業秘密使用の証拠がないため、申立人の要求は正当化できない。
IMPI の判断	申し立てを受け、相手方に対する立ち入り検査を実施。 立入を行った 7 か所のうち、4 か所からデータベースに含まれる氏名のリストが発見されたが、当該データベースとは異なっていた。 従って、営業秘密の使用を認めることはできないとして、当該請求を棄却した。

事案③

番号（EXPEDIENTE）	P.C.2147/2022(M-182)25229
結論	却下（原告からの取下げの意思表示によるため）
概要	申立人は、相手方をメキシコおよびラテンアメリカ法務責任者として雇用していた。雇用契約書には、雇用期間中および雇用期間終了後も企業秘密、営業秘密を第三者に開示してはならないと規定されていた。 更に、申立人は、社内の情報をその機密性のレベルに応じて、取り扱う情報を分類する社内システムを備えており、社内規則や情報マネジメント規定を通じて従業員全員に周知していた。 しかしながら、相手方は、弁護士やクライアントとのコミュニケーションや法的見解、第三者との契約、マーケティングや広告計画などの営業秘密を電子メールで開示していた。 このような営業秘密の開示を停止させる暫定措置を請求。

以上から、傾向を判断するには数が少ないものの、いずれも会社の労働者や元労働者が、営業秘密を流出させている事例であり、メキシコの営業秘密の流出においては、退職者を含む労働者から流出する事例が多いと考えられる。

（4）営業秘密の判例、紛争事例

メキシコにおいて、営業秘密の漏えい等、営業秘密が論点となる判例は非常に少ない。

電子登録番号（Registro digital）	2003833
区分	民事
背景	原告と被告はフランチャイズ契約を締結していた。同契約においては、商標の不使用やノウハウ、システム等の開示の禁止、競業避止などが合意されていた。 被告は、これらを遵守せず、原告は被告に対して損害賠償を請求した。
概要	フランチャイズ契約、フランチャイズ被許諾者が契約の合意事項を遵守しなかったことが間接証拠となる。 フランチャイズ契約の性質上、契約の対象となっているブランドやサービスについてフランチャイズ被許諾者が得た知識（ノウハウ）は、営業秘密として保持する義務がある。それは、フランチャイズ許諾者によって明らかにされた営業秘密によって区別される製品またはサービスの威信とイメージを直接意味するからである。フランチャイズ契約を締結することにより、フランチャイズ被許諾者は（原則として、当事者の意思に反しない限り）営業秘密の守秘義務を負い、不正競争を行わないこと、商標使用の禁止は、本契約の締結時に定められ、追加として取引契約も締結された。この考え方では、フランチャイズ被許諾者が獲得したブランドやサービスについて得た知識は営業秘密の

	保持義務を負うこととなるため、これに違反した場合には、間接証拠（推定される状況を証明すること）による証明が認められる。

（5）営業秘密管理のポイント

メキシコの「営業秘密」は、秘密に保持される産業用および商業用のすべての情報であって、①経済的価値があり、②機密性が維持され、③機密に保つための合理的措置が施されている情報となる。

また、営業秘密保有者が第三者に情報を開示するような（知識や技術を提供するような）契約では、営業秘密の保持に関する条項を設けることができ、その条項では、秘密情報を特定しなければならない。

連邦労働法に視点を移すと、労働者の義務として「直接的または間接的に生産に関与している製品の、または業務上知ることとなった技術的、商業的、製造上の秘密、および公開すると会社に損害を与える可能性がある機密事項（asuntos administrativos reservados）を厳重に管理すること」と規定されており、使用者が責任を負うことなく労働者を解雇できる事由として「労働者が製造上の秘密を漏えいし、または、会社に不利益をもたらす機密事項を漏えいした場合」と規定されるが、解雇の正当事由の責任は使用者にあるとされることから、当該情報が秘密であったこと、当該情報がその労働者によって漏えいされたことが証明できるように備えておくことが推奨される。

第Ⅱ部. 漏えい対策実践

（1）営業秘密管理の 3 ステップ

営業秘密の管理においては、メキシコ人労働者についても把握しておくことも必要である。メキシコでは、コミュニケーションアプリ（特に WhatsApp[iii]）の活用も活発で、業務上の連絡や取引先との連絡においても、コミュニケーションアプリを用いる例が非常に多い。コミュニケーションアプリによる通話やメッセージのやり取りのほか、データの授受も行われているのが現状である。また、記憶することやメモを取ることの代わりに、記録としてスマートフォンのカメラで写真を撮ることも頻繁に行われている。さらに、一般に、メキシコ人の離職率は高く、労働者の入れ替わりが激しいと言える。営業秘密管理においては、このような状況も考慮する必要がある。第 1 部から分かるように、メキシコの営業秘密に関する法制度は緻密ではない。また、営業秘密の管理について、公的機関からガイドライン等は発行されていない。しかしながら、その管理体制がメキシコと日本とで大きく変わるものではないため、日本の経済産業省が策定する「営業秘密のハンドブック～企業価値向上に向けて～（令和 4 年 5 月改定版」[iv]（以下、「ハンドブック」）を参照しながら、管理ステップを検討したい。

ステップ 1　保護すべき情報の選定および重要度の選別（参考：ハンドブック 8～16 ページ)

まず、保護すべき情報を特定し、そのような情報がどの程度の保護に値するかとの識別を行う。

i）会社が保有する情報の把握

・情報が記録される媒体にこだわらず、網羅的に把握する必要がある

・個人の感覚による判断のばらつきがないよう、経営責任者や情報管理部門責任者等による把握など、統一的な判断が可能となるような把握の方法をとる

ii）情報の評価・重要度の選別

・情報が生み出す経済的価値、漏えい等生じた際に被る損失（社会的信用の損失なども含む)、競合他社にとっての有益性、取引先への影響などを考慮し、重要度を選別する

また、企業活動においては、日々の業務の中で、情報にアクセスをせざるを得ない。併せてどの程度の範囲で共有される情報かを把握し、情報の重要度に応じてアクセス基準を定めることも有益である。

このように把握した情報は、責任管轄部署ごとにリスト化し、定期的な見直しを行い、また、管理責任者でも、これを把握しておくことが望ましい。

〈参考：保有情報チェックリスト例〉

部署（分類）	情報	重要度
技術部門	●●製品の設計図（書面）	部外秘
	●●製品の設計図（CD-R）	部外秘
	●●製品の製造工程（ノウハウ）	部外秘
	●●製品の原料配分データ	部外秘
営業部門	サプライヤー単価リスト	社外秘
	顧客リスト	社外秘
	クライアント●●製品に係る開示情報	部外秘 （関連部署含む）
管理部門	投資計画表	社外秘
	次期決算試算表	部外秘
管理部門	投資計画表	社外秘
	次期決算試算表	部外秘
		…など

ステップ２　現状の管理体制の確認

次に、現在の管理体制を把握し、情報管理の観点から脆弱な点を洗い出す作業を行う。各企業の事業内容、保有する秘密情報の種類などによって、チェックポイントは異なってこようが、次のようなセルフチェックシート作成し、検証することが有益である。

〈参考：セルフチェックシート例〉

カテゴリー	チェック項目	評価
管理方針・体制	情報管理責任者、情報管理担当部署等を設けている。	
	営業秘密管理規程や管理マニュアルが策定されている。	
	各拠点において、営業秘密管理責任者を選任している。	
	下記各項目について定期的に見直し、最新の状況を把握している。	
	規定やマニュアルは、適宜更新されている。	
秘密の特定	秘密保持の対象となるような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。	
物理的管理	外部者の入退出管理を行っている。	
	外部者が立ち入る際には、外部者と認識できるようバッジ等をつけている。	
	ミーティングルームと執務室のエリアを分けるなど、部外者が立ち入ることのできるエリアを限定している。	
	記録媒体に「Confidencialidad」など秘密であることの表示がされている。	
	一般情報と区別し、管理されている。紙媒体等を施錠管理している。	
	プリンターの利用記録が確認できる。	
	複製を制限する措置がとられている。	
	持ち出しや返却の記録が作成されている。	
	持ち出しの際の盗難防止対策がとられている。	
	生産・製作現場の様子が外部者に見えないよう適切に仕切られている。	
	生産・製作現場内では携帯電話の使用が禁止・制限されている。もしくは、使用できる労働者が限定されている。	
	重要度の高い秘密情報を取り扱うエリアへのアクセスを制限している。	
	アクセス制限エリアについて、入退室記録をとるなど、適切に管理している。	
	重要度の高い秘密情報があるエリアには監視カメラを設置している。	
技術的管理	保有する電子データをサーバー上で管理し、アクセスログを記録している。	
	秘密情報を管理する PC に外部からのアクセスに対する防護策をとっている。	
	労働者の PC にパスワードが設定されている。	
	PC のパスワードは定期的に変更されている。	
	PC の社外持ち出しを管理している。	
	PC の公共ネットワークへの接続を禁止・制限している。	
	チャットアプリの使用を禁止・制限している。	
	私物の USB 等の記録媒体の使用を禁止・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。	
	メール送信記録やウェブサイトの閲覧履歴を確認できる。	

	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	入社時やその後も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。	
	営業秘密に関し秘密保持契約を締結している（雇用契約書に規定を設けている。）	
	守秘義務に違反した際の懲罰規定が明記されている。または、これを周知している。	
	退職者による資料等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。	
	開示した秘密情報の返還や廃棄を管理している。	

ステップ３　対象別の体制整備

営業秘密の管理体制は、情報取扱責任者およびその担当部署等を設置し、営業秘密の使用、アクセス、または処理について、さらにその損傷、損失、改ざん、あるいは破壊から保護するために、物理的、組織的、および技術的な安全管理措置を実施しることが考えられる。

i）　物理的安全管理措置

物理的安全管理措置とは、営業秘密への物理的接触を制限する措置であり、情報を保存する機器やメディア、ファイリングキャビネット、引き出し、棚、倉庫などの物理的な設備や機器へのアクセスは、情報の取扱担当者にのみ許可し、その立場や機能に基づいて正当な理由がない第三者にアクセスを許可しないこと。また、それらにアクセスするための鍵やパスワードがある場合は、安全な場所に保管し、第三者に貸与または提供しないこと、営業秘密の確実な削除などが挙げられる。

ii）組織的安全管理措置

組織的安全管理措置とは、組織体制の整備や従業員の教育といったものであり、組織レベルでの情報セキュリティの管理、維持、監査体制の確立、営業秘密の識別と分類、各担当者の識別、各担当者の責任と権限の明確化、教育などが考えられる。

iii)技術的安全管理措置

情報システムの使用やシステムへの不正アクセスによる情報漏えいを防止するための措置であり、データベース等へのアクセス制御、アクセス者の識別や認証、追跡、安全なシステムの開発、運用、保守などが考えられる。

以上を踏まえ、対象別の対象整備について検討する。

（ア）　情報管理体制の専門部署/担当者の設置

営業秘密の管理においてまず必要となるのが、営業秘密の管理を担当する責任者、部署、担当者の設置であり、最善は、専門の部署を設置し、責任者と担当者を置いて、管理を行うことである。

しかしながら、メキシコ現地法人においては、日本の親会社等と比較すると、その規模が小さく、専門部署を設けることは現実的に難しい場合が多いのではないだろうか。この場合、現地責任者として赴任する駐在員等が、営業秘密管理の責任者も兼任することが考えられるが、会社のすべての管理責任者として機能していることから営業秘密の管理について能動的に動くことができない場合が多いのも現状のように見受けられる。このような場合には、日本親会社の営業秘密の管理部門からの支援を受けながら、管理体制の構築と実践を進めることが考えられる。

また、担当者についても、専門部署の設置が難しい場合は、各部署や部門ごとに担当責任者を任命し、管理を図ることが考えられる。このような場合には、担当責任者向けの研修の機会を設けたり、担当責任者同士でミーティングの機会を設けたりしながら、横断的な意識・情報共有を行うことで、より効果的な体制作りが期待できる。

また、管理体制の構築には、営業秘密保護管理の方針や具体的な方法を文書化した、情報管理規定の策定することが望ましい。メキシコ現地法人においては、日本の親会社が策定し運用する規定類をそのまま適用する例も見受けられるが、そのような場合には、全ての労働者が理解できるよう、メキシコ人になじみのある表現等を用いたスペイン語版を用意し、運用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

従業員の管理の要は、従業員に守秘義務を課すことである。その対象は自社で雇用する労働者はもちろん、労働者派遣(subcontratación de personal)のサービスを受ける場合は、その労働者も対象とする必要がある。後者については、派遣元企業との契約において、当該派遣労働者に秘密保持義務を課すこと、当該派遣労働者にも自社の営業秘密規定に従う必要があることの教育や、自社の営業秘密に関する研修を受講させることなどを約束する条項を設けるなどして、その管理体制の対象とすることが考えられる。

●入社時

労働者とは雇用契約書を締結することとなるが、その中で労働者に対して秘密保持義務を課すことや別途秘密保持契約を締結することが考えられる。前述のとおり、メキシコの連邦労働法では、業務上知ることとなった技術的、商業的、製造上の秘密、および公開すると会社に損害を与える可能性がある機密事項を厳重に管理することが労働者の義務として規定されてはいるが、これを意識できているメキシコ人労働者はそれほど多くないと考えられる。また、労働者本人が、会社のどの情報が「機密事項」に該当するのか認識できなければ、その機密を保持できない。従って、秘密保持条項や契約書において、秘密保持の対象となる情報の具体例を提示することが推奨される。また、この会社に損害を与える可能性がある機密事項を漏えいし

た場合は、正当な解雇事由に該当するのであるが、これを認識している労働者も少ないと考えられ、雇用契約書や秘密保持契約書においても、漏えいが解雇事由にあたることを確認することが望ましい。さらに、法の規定にも触れ、機密漏えい時には、会社が民事、刑事措置をとることができ、損害賠償請求の可能性があることも規定したい。

●在職中

労働者に対しては、その職務に応じた適切なアクセス権限の付与が重要である。秘密情報を閲覧・利用等することができる者の範囲を適切に設定した上で、該当者への ID の付与などを行い、また人事異動時には直ちにその権限の変更や ID の削除などを行う必要がある（参考：マニュアル 38～44 ページ)。

特に、テレワーク労働者については、外部から社内ネットワークへのアクセスを行うことから、アクセス権限の細かい設定など考慮する必要がある。

また、定期的な営業秘密保持研修の実施も不可欠である。この場合、労働者の十分な理解や意識付けのためにも、スペイン語の資料によるスペイン語での実施が望ましい。なお、前述のとおり、業務においてのコミュニケーションアプリの活用は活発であり、これを禁止することは難しいと考えられる。会社から貸与された携帯電話端末であっても、個人のアカウントを用いて、私的に利用する例もあることから、定期的な研修において、細かく教育する必要がある。

また、内部通報窓口の設置やその周知の徹底も不正の予防、早期発見につながる。この内部通報窓口はメキシコ現地法人独自に設ける場合のほか、日本の親会社等がグループ全体に対して設ける窓口を活用する方法が考えられる。

●退職時

退職時には、在職中に管理していた営業秘密関連書類や資料、業務用パソコン等の機器をすべて回収し、当該労働者が使用していたアクセス ID や電子メール ID を直ちに削除しなければならない。

退職者が勤務当時に接した情報の範囲を特定しやすい。このことから、退職者に対して、守秘義務のある営業秘密の種類を特定した営業秘密保持契約書締結することや退職合意書内で同等の条項を設け、合意を取っておくことが望ましい。

なお、メキシコにおいては、就業および職業選択の自由はメキシコ合衆国憲法（Constitucón Política de los Eestados Unidos Mexicano）5 条に保障される基本的人権と考えられていることから、競業避止義務を課すことはできないとの考えが一般的のようであるが、雇用契約書や退職合意書において、退職後の競業避止義務を規定するものも見受けられる。真の意味で労働者に競業避止義務を課す場合は、相当の対価を求められることも考えられる。

（ウ） 執務室の管理

●立入の制限

入口付近に会議室や面会場所などを設置し、来訪者等の外部者が社内になるべく立ち入らない構造とする。また、外部者の来訪は事前予約制とし、来訪時には、受付にてその人の身分（氏名、会社名など)、訪問目的、訪問対象者などを記録するようにし、外部者であることが分かるように入館証を携帯するようにする。

アクセス制限と入退出記録を行えるよう、執務室入口は ID カードなどを用いて開錠できる施錠システムを設けることが望ましい。また、廊下や駐車場などから執務室を覗くことができる場合は、窓にブラインドなどを設置する。

●資料の管理

秘密情報を含む紙などの物理的媒体には、「Confidncialidad」など秘密であることが分かるよう表示を行う。

また、その管理は、一般の資料とは区別し、施錠のできるキャビネットや金庫で保管するようにし、その鍵や資料の持ち出しと返却については、日時や持出者の氏名などを記した記録を作成する。

また、プリンターや複合機は、利用履歴を確認できるものを使用する。

サーバーや書庫等、執務室とは異なるエリアに営業秘密が保管される場合は、その入り口を ID カードなどで開錠できる施錠システムを設け、入退室管理を行い、持ち出しがある場合は、同様に持ち出しや返却の記録を作成する。また、入口付近などに監視カメラを設置することも推奨される。

秘密の重要度に応じて、営業秘密を含む資料を外部に持ち出す場合には、申請をし、許可を得て持ち出す制度を設けることも考えられる。

●廃棄

営業秘密を含む資料などが不要となった場合は、直ちに、復元できないよう破壊し、廃棄する。

（エ） 生産現場の管理

●立入の制限

執務室同様に外部者の立ち入りについても管理を徹底する。取引先などの見学にそなえ、重要な施設へのアクセスができないよう、外部者用の制限された導線を確保する。

持ち込み・持ち出しの制限

試作品等の持ち出しを制限し、また、現場の写真や動画の流出を防ぐため、労働者の生産現場への入退場については、原則手ぶらとし、入退場の際の手荷物検査ができると望ましい。

●資料管理・廃棄

試作品等営業秘密の対象となるが生産現場にある場合は、他と区別して管理し、不要となった場合は、直ちに復元不可能な状態に破壊し、廃棄する。廃棄が直ちに行えない場合は、施錠管理などを行う。

（オ） ライセンシーの管理

社外に対して営業秘密を提示する場合には、事前に必ず秘密保持契約や秘密保持条項を含む契約書を締結し、これを締結するまでは情報を開示しないこと、必要最低限の開示にとどめる事を徹底する。また、それらの契約書においては、秘密に扱う情報を特定し、場合によっては用途を限定することも必要となる。

情報開示後に、その取引の中で不要となった情報があるときは、都度、その回収や破壊を依頼し、その証憑を取得する。

継続的な取引となるライセンシーの場合は、定期的に営業秘密保持体制の検査等を行う。

（２）関連契約書作成上の留意点

営業秘密管理の体制整備に必要となる契約書類を検討する。

●雇用契約書/守秘義務契約書

個々の労働者との間で締結する雇用契約書において、守秘義務を課すことを明記する。労働者本人が、会社のどの情報が「機密事項」に該当するのか認識できなければ、その機密を保持できないことから、秘密保持の対象となる情報の具体例を提示することが推奨される。また、前述のとおり、営業秘密の漏えいは、正当な解雇事由に該当するため、これを明記して確認すること望ましい。

雇用契約書とは別に、守秘義務契約書を締結することも考えられる。この場合も同様に秘密保持の対象となる情報の具体例を提示すること、漏えいが解雇事由に該当することを規定することが推奨される。さらに、法の規定にも触れ、機密漏えい時には、会社が民事、刑事措置をとることができ、損害賠償請求の可能性があることも規定したい。

●退職合意書

退職合意書内に、守秘義務のある営業秘密の種類を特定した営業秘密保持義務を記載し、合意を取っておくことが望ましい。また、営業秘密の内容に合わせて退職後の守秘義務期間を設けることも考えられる。

メキシコでは、競業避止義務を課すことはできないとの考えが一般的であるため、競業避止義務の規定には配慮が必要である。当事者が合意できれば、単に抑止力として規定を設けることも考えられる。違反時に制裁金を科す規定を設けるなど、真の意味で労働者に競業避止義務を課すような場合は、相当の対価を支払うことも検討する必要があろう。

●就業規則

単に営業秘密の保持を規定するだけでなく、例えば、「事前の承諾を得ずに業務に関係のない第三者を会社の敷地内に招き入れてはならない」など営業秘密保持体制の維持に必要な条項を設け、これらの違反に対する懲罰を定めることが推奨される。

●情報取扱規定

会社において営業秘密を管理する部署や役職に関する規定や会社が秘密情報として取扱う情報の類型や重要度、管理方法、アクセス権限の範囲について規定する。

●取引先等との秘密保持契約書

企業間で新たに営業秘密が開示される場面においては、必ず秘密保持契約を結ぶべきである。具体的には、共同開発事業の検討開始時、新たな取引の開始検討にあたって非公開の商品情報や価格、生産計画などを開示する場合、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検討・依頼する場合、M&A やそれに先立つデューデリジェンスの実施などが想定される。契約書には、一般には、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および目的外利用の禁止、秘密情報の開示がそのライセンスや譲渡等を意味するものではないこと、秘密情報の破棄・返還に関するルール、情報漏えい時の通知義務等が規定される。既に具体的な事案について、取引の開始が決まっている場合には、これらを秘密保持契約書としてではなく、取引基本契約書等の取引に関する契約書内に記すことも考えられる。

●フランチャイズ契約

法では、フランチャイズについても規定している。法 248 条は「*フランチャイズ被許諾者は，契約の期間内及び終了後，当該契約に基づき遂行される経営及び活動に関する情報を含み，秘密性のある情報，知り得た情報又はフランチャイズ許諾者の財産である情報の秘密性を保持しなければならない*」と規定する。

アンパロ裁判において裁判所が示した基準では、フランチャイズ被許諾者がフランチャイズ契約に係る情報を無断で第三者に開示した場合、フランチャイズ許諾者は、フランチャイズ契約の存在を以て、その個別具体的な事例を証明することなく、第三者に開示したと推定される状況を証明するのみで足りるとされている（Amparo directo 406/2011、Reistro digital: 2003833[v]）。このように法で保護されてはいるものの、機密性のある情報の特定、その利用目的、利用範囲、守秘義務などを記すことが推奨される。

（３）漏えい事案への対応

（ア）漏えい兆候の把握（参照：ハンドブック 145～147 ページ）

漏えい兆候の把握の方法については、ハンドブックに具体例が多く掲載されている。これらも参照しつつ、メキシコ人の傾向を踏まえながら、漏えいの兆候を例示する。

●従業員等の兆候

・（業務上の必要性の有無に関わらず）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（担当業務外の情報が保存されたサーバーやフォルダへの不必要なアクセス、不必要な秘密情報の大量ダウンロード、私物の記録媒体等の不必要な持込みや使用）
・自身の業務と関係のない部署への頻繁な出入り
・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
・急激に浪費をし始めた
・業務用 PC や携帯電話の会社へのメンテナンス等による引渡しの拒否
・労働者自身による不要なパスワードの設定、変更
・他の労働者との交流が少なくなった（接触を避けている）
・給与の引き上げの要請があったが応じなかった

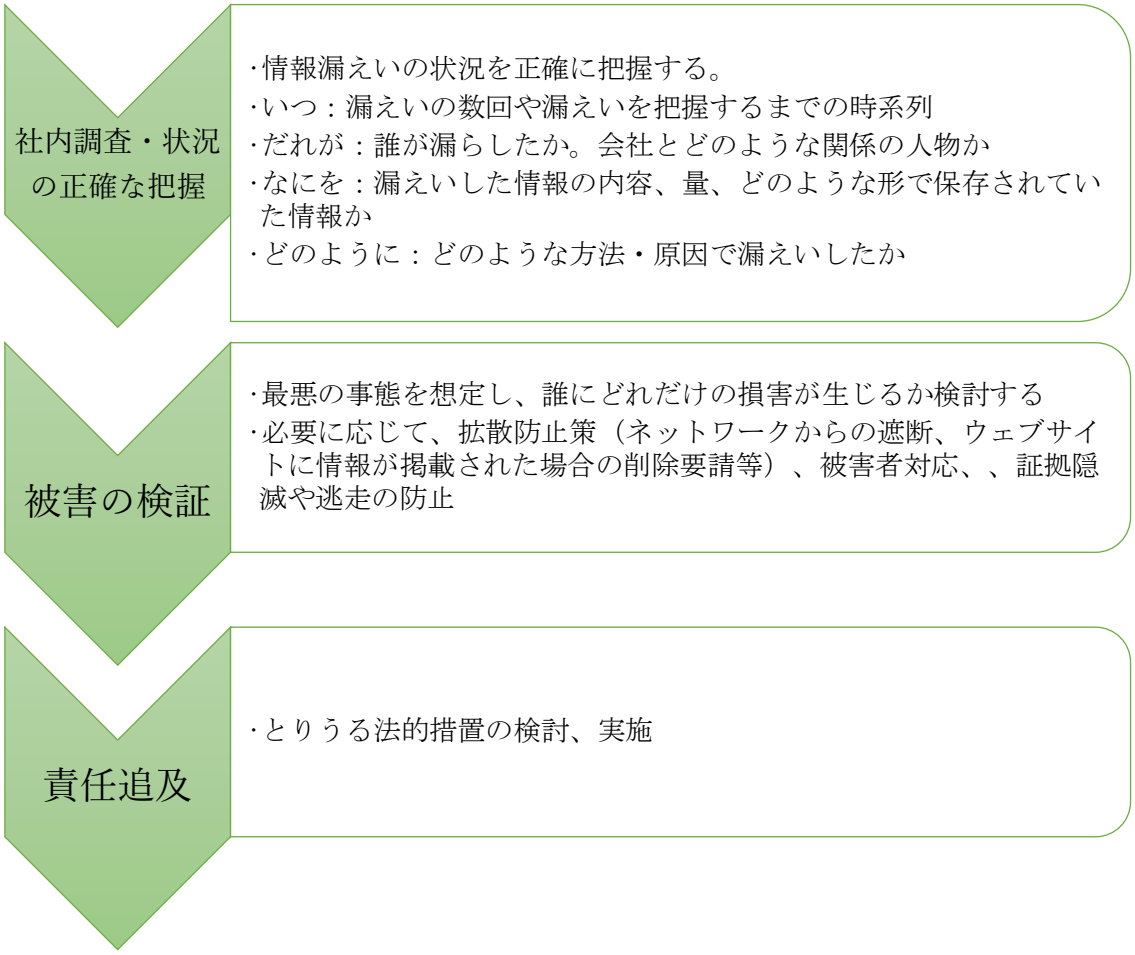
●退職者の兆候
・退職前の社内トラブルの存在
・競合他社から転職の勧誘を受けていた
・元従業員の不審な言動が同僚内の会話で話題になっている
・退職者の転職先企業が製造・販売を開始した商品の品質や機能が、特に転職後、自社商品と同水準となった

●取引先の兆候
・取引先からの突然の取引の打切り
・インターネット上での取引先に関する噂
・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要請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
・取引先からの異様なほどまでの訪問回数の増加

●外部者の兆候
・自社における社員証・パスワードなどの流出、オフィスにおける盗難などの事件の発生
・自社会議室における偵察機器（盗聴器など）の発見
・競合他社等での秘密情報漏えい、不法侵入等の事案発生
・ウィルス対策ソフト、セキュリティ対策機器による警報
・自社の秘密情報それ自体ではないが、それと不可分一体のはずの情報が漏えいしていること
・電話、メール等を受信した関係者からの通報 ex）自社の顧客名簿に記載された者が、競合他社から営業の電話を受けたが、その競合他社に連絡先を教えた覚えがないため、不審に思ってその旨連絡をしてきた

（２）初動対応（参考：ハンドブック 151～154 ページ）

漏えいの兆候が見られた場合、速やかに事実関係を調査・確認し、被害の拡大防止、企業イメージの保護、迅速かつ適切な法的措置のために、適切な初動をとることが重要となる。



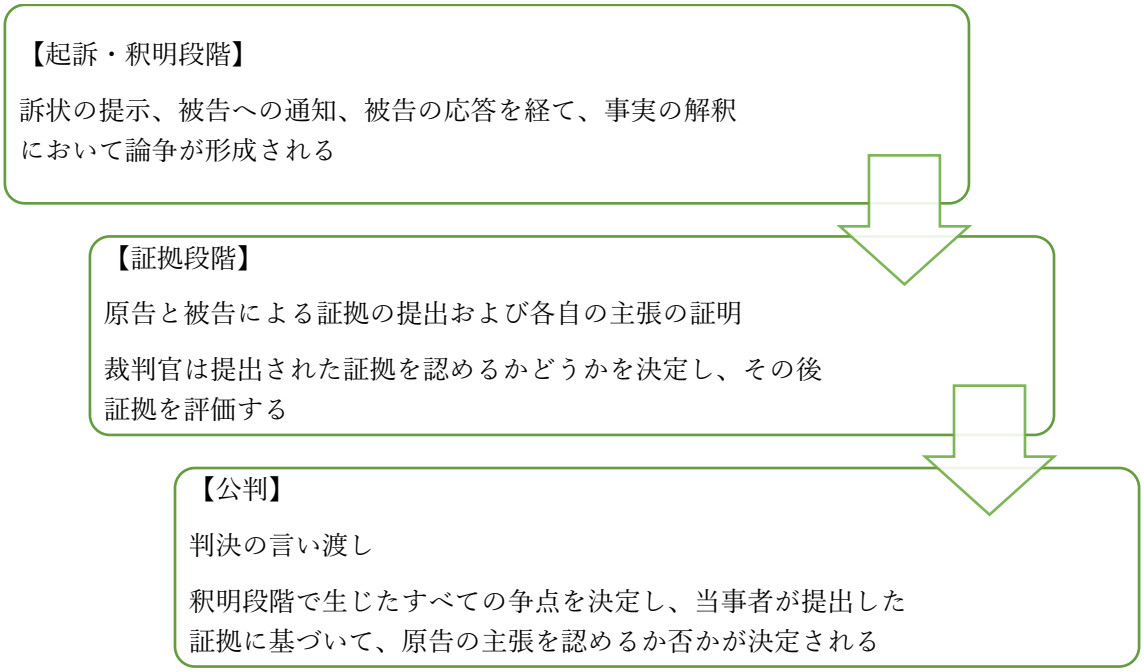
（３）民事措置

営業秘密の漏えいによる営業秘密保有者の権利侵害に対しては、賠償金が請求できる。その賠償金は、対応する行政手続きを経た後に IMPI に対して申し立てる方法と、直接、連邦レベルの民事裁判所に申し立てる方法が認められる（法 396 条、407 条）。通常の民事裁判として、賠償金を請求する場合、被告に権利侵害行為があったことを原告が証明する必要があることから、単に民事手続きのみで賠償金請求を行うことは非常に難しいと考えられる。

なお、賠償金については、侵害の結果、営業秘密所有者は、証拠と併せて、受け取ることのできなかったであろう利益や違反者が侵害の結果得た利益をもととした価値の指標を提示し、これを考慮し決定される。なお、賠償金額は、営業秘密保有者が提示した指標額の 40%を下回ってはならないこととなっている（法 396 条、397 条）。

民事訴訟の流れは以下のとおり。

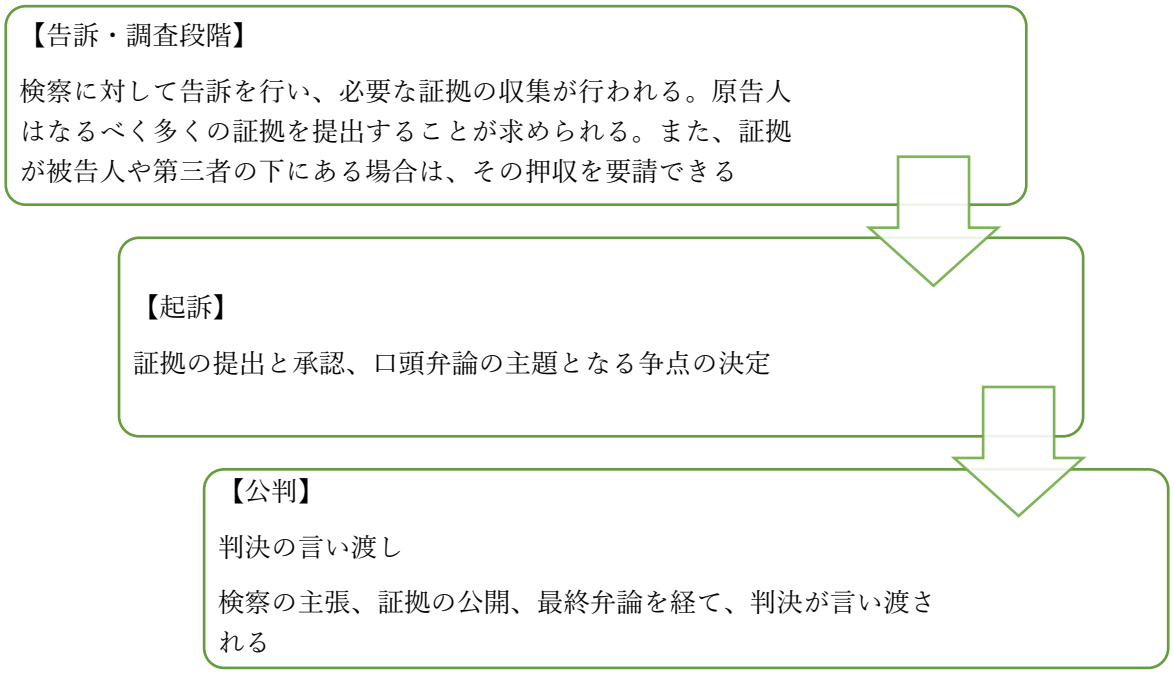
なお、営業秘密の漏えい関する証拠が、被告や第三者の手元にある場合、原告はその所在を明らかにして、裁判所に対して、当該被告や第三者にそのような証拠を開示させることを請求することができる。



（4）刑事措置

刑法あるいは法の規定に基づく刑事告訴の措置も取られうる。

流れは次のとおり。



（５）行政措置

前述のとおり、法では、営業秘密に関連する２つの行政違反行為が定められている。１つ目は営業秘密の流用であり、2 つ目は営業秘密を使用する製品またはサービスの製造、販売、輸入、輸出、または保管である。この違反について、営業秘密保有者や使用者は IMPI に対し行政違反の宣言を申請することができる。なお、この行政違反の宣言は申立のほか、職権でも開始することができるとなっているが、実際に職権で行われることは極めて少ないと考えられる（法 328 条、329 条）。

行政違反宣言の判断においては、両当事者がそれぞれの主張を証明する十分な証拠を提出しなければならない。証拠が相手方当事者の下にあることを示して証拠として言及した場合、IMPI は当該相手方当事者に対して、十分な機密保持の配慮を行った上でこれを開示させることができる（法 334 条）。IMPI は当事者の主張と証拠を審査し、課される制裁を含めた行政決議を発行する。なお、該当する場合には損害賠償も決議に含まれる場合がある（法 342 条、343 条）。

また、IMPI は、当該違反に関連し、商品等の流通の停止や輸出入・通関手続きの停止を命じることができる（法 344 条）。

（６）行政手続きにおける調停

行政違反宣言の申立てが行われてから決議が発行されるまで、当事者はいつでも調停を申し出ることができる。調停では、IMPI は裁定を下すことなく、当事者は自身の責任で合意を採択することとなる（法 372 条、373 条）。

（７）仲裁

営業秘密の漏えいに関し、仲裁による解決を図ることも考えられる。メキシコにおける仲裁は商法（Código de Comercil）に規定されている。仲裁機関は、国際商業会議所（International chamber of commerce）やメキシコ仲裁センター（Centro de Arbitraje de México)、メキシコシティ商工会議所(Cámara Nacional de Comercio de la Ciudad de México)等が存在する。

仲裁合意は書面においてなされなければならない（商法 1423 条）。従って仲裁による解決を図るためには、その解決方法について当事者の合意が必要となることから、あらかじめ契約書においてこれを定めておくことが望ましい。

仲裁廷は、紛争を解決するために指名された 1 名または複数の仲裁人となる。仲裁人の人数は当事者の合意により自由に決定することができるが、このような合意が存在しない場合には仲裁人は１名となる（商法 1416 条、1426 条）。

仲裁人の選任は、当事者間で自由に合意することができる。この場合、仲裁人の国籍も問われない。仲裁人の選任について合意がない場合や単独仲裁人による仲裁において当事者が仲裁人の選任について合意できない場合は、裁判官が、当事者の請求により、仲裁人を選任する。3 名の仲裁人を置く仲裁においては、各当事者は、1 名の仲裁人を選任し、選任された 2 名の仲裁人が、3 人目の仲裁人を選任する（商法 1427 条）。

仲裁廷が従うべき手続、仲裁の場所、使用言語も当事者の合意により決定することができる（商法 1435 条、1436 条、1438 条）。

当事者による別段の合意がない限り、仲裁廷は、証拠の提示・口頭弁論期日を設けるかどうかを決定する。ただし、仲裁廷は、当事者が口頭弁論期日を設けないと合意しておらず、当事者のいずれかから要求があった場合には、手続の適切な段階で口頭弁論期日を設けなければならない（商法第 1440 条）。

なお、仲裁手続の秘密保持や非公開については規定がない。商法 1435 条は、仲裁手続を決定するための幅広い裁量を当事者に与えており、当事者は、仲裁を秘密にするかどうかを決定する権限を持っていると考えられ、当事者が仲裁合意において非公開を合意した場合は、仲裁人を含めてこれに拘束されると解される。

仲裁判断は書面として作成され、仲裁人により署名がなされる。当該書面には、当事者が別段の合意をしている場合、または和解合意の場合を除き、その判断の根拠となる理由が記載される（商法 1448 条）。

仲裁手続中に当事者が和解に至った場合、仲裁廷は手続を終了する。この時、当事者双方から申出があり、仲裁廷が特段問題ないと判断する場合には、仲裁判断の形式で和解を記録する（商法 1447 条）。

仲裁判断は、いずれの国で為されたかを問わず、拘束力を有するものと認識され、その執行は、仲裁判断が記された書面および仲裁合意が記された書面の原本または認証謄本（copia certificada）をもって、裁判所に書面をもって請求する。なお、仲裁判断や仲裁合意がスペイン語で記されていな場合は、認証翻訳者（perito traductor）による翻訳を添付しなければならない（商法 1461 条）。仲裁地がメキシコ国内だった場合は、その仲裁地を管轄する連邦または州の第一審裁判所の裁判官が、仲裁地がメキシコ国外だった場合は、執行を受ける当事者または対象の資産の所在地を管轄する連邦または州の第一審裁判所の裁判官となる（商法 1422 条）。

仲裁費用について、当事者は仲裁規則に従う旨の合意をすることが可能である（商法 1452 条）。

当事者の合意がない場合、仲裁廷は仲裁判断において仲裁費用を定める（商法 1453 条）。仲裁廷の費用は、係争額、案件の複雑さ、仲裁人が費やした時間その他関連する事情を考慮して決定される。また、各仲裁人の報酬は、仲裁廷によって決定される（商法 1454 条）。

このような費用は、原則、敗訴した当事者が負担することとなるが、仲裁廷は、事件の状況を考慮し合理的と判断した場合には、仲裁費用を両当事者に負担させることができる（商法 1455 条）。

例えば、メキシコ仲裁センターの場合、係争金額に応じて、管理費や仲裁人費用が定められており、CAM のホームページ[vi]で確認することができる。2022 年 12 月 1 日以降の仲裁合意に基づく仲裁については、200 万ペソの係争金額の場合、管理費として 4 万 9,600 ペソ、仲裁人費用として 9 万 7,840 ペソと算出される。

（８）証拠の保全（参考：ガイドブック 159～160 ページ）

電子情報など、証拠の種類によっては時間の経過とともに失われるものもあり、迅速な証拠の保全が求められる。特に労働者による漏えいが疑われる場合、会社の対応などを見ながら、証拠の隠滅が行われることも考えられる。漏えいの兆候から初動対応等への各過程において、証拠となるものを確実に収集していくことが求められる。

また、状況に応じて、、デジタルフォレンジック等専門家との協力も有効である。

【参考資料：各種関連書類参考書式（フォーム）】

（ア）就業規則（参考和訳付き）

Confidencialidad

Artículo ●: El trabajador se compromete a guardar escrupulosamente los secretos técnicos comerciales y/o de fabricación de los productos a cuya elaboración concurra directa o indirectamente, o de los que tenga conocimiento por razón del trabajo que desempeña, así como de los asuntos administrativos reservados y cuya divulgación pueda causar perjuicios a la Empresa.

秘密保持

第●条：労働者は、生産に直接的または間接的に関わる、または自身が行う業務により知り得た製品の技術的、商業的および/または製造上の秘密、および開示することによって会社に損害を与える可能性のある秘密情報を厳重に保持しなければならない。

Derecho y Obligaciones de los Trabajadores

Artículo ●: Son obligaciones de los trabajadores:

…

- Guardar escrupulosamente los secretos técnicos y comerciales de los cuales tengan conocimientos por razón del trabajo que desempeñan, tanto de la empresa como de terceros que esta tenga derecho de usar, así como de los asuntos administrativos

reservados, cuya divulgación pueda causar perjuicios a la empresa o a cualquier tercero.

…

労働者の権利・義務

第●条：労働者は次の義務を負う。

…

● 職務上知りうる技術的・商業的秘密、会社および会社が使用権を有する第三者の機密、その他公開すると会社または第三者に対して損害を引き起こす可能性のある秘密情報を厳重に保護すること。

…

Artículo ●: Queda prohibido a los Trabajadores:

…

- Entrar a las instalaciones de la empresa después de las horas de labores, sin la previa autorización de su Jefe Inmediato Superior.
- Fumar o usar teléfono celular, fuera de las áreas designadas para tal efecto.
- Efectuar trabajos personales a clientes de la Empresa o terceros dentro de las horas de trabajo o cuando se encuentre el Trabajador ejecutando alguna labor encomendada por la Empresa.
- Sustraer de la Empresa útiles de trabajo, materiales u objetos que no le pertenezcan, sin permiso y/o procedimiento autorizado por la Empresa.
- Introducir a las instalaciones de la Empresa, sin autorización, a personas u objetos extraños.

…

第●条：労働者は次の事項を行ってはならない

…

- 直属の上司の許可なく、勤務時間後に会社の施設に立ち入ること
- 決められた場所以外で、喫煙や携帯電話を使用すること
- 勤務時間内、もしくは会社から指示された業務を行っているときに、会社の顧客や第三者のための個人的な業務を行うこと
- 会社の許可を得ず、または会社が定めた手続きを経ずに、自身の所有物ではない会社の工具、資材等を持ち出すこと
- 許可なく、外部の人や物を会社の施設内に招きまた持ち込むこと

…

Medidas Disciplinarias y Sanciones

Artículo ●: Sin defecto de lo dispuesto por el artículo 47 de la LEY, será motivo de rescisión de la relación de trabajo la infracción a las fracciones ●, ●, ● del articulo ● y las fracciones ●, ●, ●,● del articulo ● del Presente Reglamento.

懲戒処分と懲戒

第●条：法第 47 条の規定に反しない限り、本規定の第●条第●、●、●号、および第●条第●、●、●号の違反は、雇用関係終了の事由となる。

なお、メキシコにおいて就業規則の制定は義務とはなっていないが、就業規則を定めた場合は、使用者の代表者と労働者の代表者からなる混合委員会（Comision Mixta）にて承認し、両当事者が合意した場合は、署名後 8 日以内に連邦労働調停登録センター（Centro Federal de Conciliación y Registro Laboral）に届出なければならない（連邦労働法 424 条）

（イ）従業員との秘密保持契約書（参考和訳付き）

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN CELEBRADO EL [*DD MM DE AAAA*], ENTRE [*Nombre de Empresa*], EN ADELANTE "LA EMPRESA", REPRESENTADA POR EL C. [*Nombre de Representante Legal*] Y EL C. [*Nombre de Trabajador*], EN ADELANTE "EL EMPLEADO", A QUIENES CONJUNTAMENTE SE LES DENOMINARÁ LAS "PARTES", Y QUE ESTÁN OBLIGADAS AL TENOR DE LAS SIGUIENTES DECLARACIONES Y CLÁUSULAS:

（法定代理人氏名）が法定代理人を務める(会社名)（以下、「会社」）と（従業員氏名）（以下、「従業員」）（総じて「両当事者」）は、（年月日）に秘密保持契約を締結し、以下の各条項に拘束される。

DECLARACIONES DE LA EMPRESA:

I. LA EMPRESA declara, a través de su representante legal, que está legalmente constituida bajo las leyes mexicanas y tiene su domicilio en: [*Domicilio*] y se encuentra inscrita en el Registro Federal de Contribuyentes del Servicio de Administración Tributario dependiente de la Secretaría de Hacienda y Crédito Público, con el número [*RFC*].

II. LA EMPRESA declara que su representante legal tiene poderes suficientes para celebrar el presente Acuerdo.

「会社」による宣言

I. 「会社」は、メキシコの法律にもとづき設立されており、（住所）に所在し、大蔵公債省国税庁に（納税者番号）にて納税者登録されていることを証する。

II. 「会社」は、その法定代理人が、本契約を締結するために必要な権限を有することを証する。

DECLARACIONES DEL EMPLEADO:

I. EL EMPLEADO declara que firma el presente Acuerdo otorgando su voluntad, con sus facultades mentales.

「労働者」の宣言

I. 「従業員」は、自らの意思でこれに署名することを証する。

DECLARACIONES DE LAS PARTES:

I. LAS PARTES mantienen actualmente una relación laboral.
II. LAS PARTES reconocen la personalidad con la que comparecen en la firma del presente Acuerdo.

両当事者の宣言

I. 両当事者は、現在雇用関係を有する。
II. 両当事者は、本契約を締結する際にどのような人格を有するかを確認した。

CLÁUSULAS
条項

PRIMERA.
OBJETO DEL ACUERDO DE CONFIDENCIALIDAD
El presente Acuerdo tiene como objetivo proteger la información que pertenece a LA EMPRESA y establecer los términos y condiciones bajo los cuales EL EMPLEADO mantendrá la confidencialidad de los datos e información, ya sea de forma oral, gráfica, escrita u otros; transmitidos o divulgados por LA EMPRESA u obtenidos o revelados a través de actividades laborales bajo LA EMPRESA.

第一条
本契約の目的
本契約の目的は、「会社」に属する情報を保護し、「会社」が開示し、または「会社」における業務を通じて取得もしくは開示を受けたデータおよび情報であって、口頭、図面、書面等の形態を問わず、「従業員」がこの機密性を維持するための条件を確立することである。

SEGUNDA.
INFORMACIÓN CONFIDENCIAL

Se considerará Información Confidencial cualquier información perteneciente a LA EMPRESA u obtenida por LA EMPRESA de sus clientes, proveedores, vendedores o cualquier otra persona, que no sea de conocimiento general en la industria o por el público, cuya divulgación podría resultar perjudicial para LA EMPRESA, sus empresas matrices, empresas subsidiarias o empresas afiliadas. Incluye, entre otros, información técnica, información industrial, información financiera, proyecciones y pronósticos financieros, conceptos, ideas, conocimientos, técnicas, know-how, planes de negocios, diseños, dibujos, borradores, diagramas, textos, modelos, muestras, bases de datos, programas, aplicaciones, listas de precios, planes y estrategias, costos, listado e información de clientes, información de proveedores y vendedores, planes y estrategias de marketing, estudios de mercado, así como cualquier otra información de carácter personal o comercial, independientemente de su presentación o distribución. formato, ya sea oral, escrito, visual, grabado en soporte magnético o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o por conocer.

Asimismo, se considerará Información Confidencial no sólo la información que esté marcada como confidencial al momento de estar a disposición de EL EMPLEADO sino también aquella cuya confidencialidad se deduzca por la naturaleza de la información o las circunstancias que rodearon la información.

Este Acuerdo y cada cláusula del mismo también son Información Confidencial.

Información Confidencial no incluye información que ya está disponible al público sin acto ilícito o incumplimiento por parte de EL EMPLEADO, que pasa a estar disponible al público sin culpa alguna de EL EMPLEADO, o que debe divulgarse de conformidad mediante orden judicial o de autoridad gubernamental, siempre que EL EMPLEADO notifique prontamente a LA EMPRESA de dicha solicitud.

第 2 条

機密情報

機密情報は、「会社」に属する情報、または「会社」がクライアント、サプライヤー、ベンダー、またはその他の人物から取得した情報であり、業界内または一般に知られておらず、その開示が「会社」、その親会社、子会社、関連会社に不利益となる可能性がある情報である。これには、口頭、書面、視覚的、磁気媒体に記録された、または有形か無形か、現在知られているか、または今後知られるかを問わずその他の手段また形態の技術情報、産業情報、財務情報、財務予測および計画、コンセプト、アイデア、知識、技術、ノウハウ、事業計画、設計、デザイン、図画、図表、草稿、図面、テキスト、モデル、サンプル、ベースデータ、プログラム、アプリケーション、価格表、企画戦略、コスト、顧客リストと情報、サプライヤーと販売者の情報、マーケティング計画と戦略、市場調査、その他の個人情報または商業情報などが含まれる。

同様に、機密情報は、「従業員」に提供された時点で機密としてマークされている情報だけでなく、情報の性質または情報を取り巻く状況によって機密性が推定される情報も含むものとする。
本契約および本契約の各条項も機密情報となる。
機密情報には、「従業員」の違法行為や不遵守なくして公知となった情報、「従業員」の過失なしに公知となった情報、または「従業員」がその要請を「会社」に速やかに通知することを条件として、裁判所命令または裁判所命令に従って開示する必要がある情報は含まれない。

TERCERA.
OBLIGACIÓN DE SECRETO Y CONFIDENCIALIDAD

De conformidad con la fracción XIII del artículo 134 de la Ley Federal del Trabajo, EL EMPLEADO se obliga a no divulgar ni utilizar la Información Confidencial para beneficio propio o de terceros, ya sea directa o indirectamente, y a mantener la más estricta confidencialidad de la Información Confidencial, en su caso, advirtiendo de dicho deber de confidencialidad y secreto a sus compañeros de trabajo, asociados y cualquier persona, que deba tener acceso a la Información Confidencial por su cargo o relación con EL EMPLEADO.

EL EMPLEADO se compromete a poner los medios necesarios para que la Información Confidencial no sea divulgada ni transferida. EL EMPLEADO adoptará a la Información Confidencial las mismas medidas de seguridad que a la información de su propiedad, evitando su pérdida o robo.

Además, EL EMPLEADO tiene prohibido divulgar Información Confidencial por cualquier medio, como, entre otros, publicar en redes sociales, para cualquier propósito.

EL EMPLEADO se compromete, en su caso, a advertir a sus compañeros de trabajo de la existencia del deber de confidencialidad, y a cualquier persona a quien haga accesible la Información Confidencial, responsabilizándose del uso indebido de la Información Confidencial.

EL EMPLEADO se compromete a que el uso de la Información Confidencial sólo estará encaminada a la consecución de objetivos propios de la relación laboral, y no otros, y sólo será de conocimiento para las personas estrictamente necesarias para su uso y cumplimiento.

第 3 条
機密保持義務

連邦労働法第 134 条第 13 号の規定に従い、「従業員」は、直接か間接かを問わず、自身または第三者の利益のために機密情報を開示または使用せず、機密情報の機密性を厳格に維持しなければならない。また、必要に応じて、機密情報にアクセスする必要がある同僚や関係者、その他の人物に対して、機密保持義務について警告しなければならない。

「従業員」は、機密情報が開示または譲渡されないように必要な手段を講じるものとする。「従業員」は、機密情報に対しても自分の情報財産と同じセキュリティ対策を講じ、紛失や盗難を防止するものとする。
さらに、「従業員」は、目的を問わず、ソーシャル ネットワークへの投稿などのいかなる手段によっても機密情報を開示してはならない。
「従業員」は、適宜、機密保持義務の存在を同僚、および機密情報にアクセスできるようにした人に対して警告し、機密情報の不適切な使用については責任を負う。
「従業員」は、機密情報の使用は雇用関係の目的を達成することのみを目的としており、その他の目的を達成することを目的とせず、機密情報はその使用や実施に厳密に必要な人々にのみ知られるものであること確認する。

CUARTA.
DERECHOS DE PROPIEDAD INTELECTUAL

Los derechos de propiedad intelectual de la Información Confidencial revelada a EL EMPLEADO bajo el Acuerdo pertenecen a LA EMPRESA o su propio titular y el hecho de revelarla a EL EMPLEADO bajo la relación laboral no cambiará dicha situación.

Las cláusulas de este Acuerdo no pueden interpretarse en el sentido que otorga EL EMPLEADO, explícita o implícitamente, una licencia, cesión de una patente o una patente pendiente de concesión, derechos de autor, derechos de diseños industriales y modelos de utilidad, de secretos industriales, de marcas o de know-how, o cualquier otro derecho de propiedad intelectual que se aplique a toda o parte de la información contenida en este Acuerdo.

第 4 条
知的財産権
本契約に基づいて「従業員」に開示された機密情報の知的財産権は「会社」またはその所有者に帰属し、雇用関係に基づいて従業員に開示したという事実によって当該状況が変わることはない。
本契約の条項は、明示的または黙示的を問わず、「従業員」がライセンス、特許や出願中特許、著作権、実用新案権、意匠権、商標権、工業秘密やノウハウに係る権利、または本契約に言及のある情報の全部または一部に生じるその他の知的財産権を付与されるという意味で解釈されない。

QUINTA.
DURACIÓN

Este Acuerdo entra en vigor a partir de la fecha de su firma indicada en el encabezado. LAS PARTES acuerdan que, a partir de dicha fecha, estará vigente mientras exista la relación laboral entre LAS PARTES.

Sin embargo, este Acuerdo podrá ser modificado o terminado repentinamente mediante el consentimiento expreso por escrito de LAS PARTES.

Las disposiciones relativas a la obligación de confidencialidad establecidas en este Acuerdo se aplicarán durante toda la vigencia de este Acuerdo y prevalecerán durante los 2 años posteriores a su terminación.
En relación con la Información Personal, EL EMPLEADO tiene que mantenerla estrictamente confidencial por tiempo indefinido.

第 5 条
期間
本契約は、冒頭に記された署名日から発効する。両当事者は、当該日付から両当事者間の雇用関係が存在する限り、これが有効であることを確認する。
ただし、本契約は両当事者の書面による明示的な同意によって変更または終了することができる。
本契約に定められた機密保持義務に関する規定は、本契約の有効期間中はもちろん、期間終了後も 2 年間有効とする。
個人情報に関しては、「従業員」はそれを無期限に厳重に機密として保持しなければならない。

SEXTA.
RESTITUCIÓN Y DESTRUCCIÓN DE INFORMACIÓN CONFIDENCIAL
En caso de terminación de este Acuerdo, independientemente de su causa, EL EMPLEADO se compromete a devolver toda la Información Confidencial, todas las copias del mismo y los equipos, materiales, documentos, etc. que contengan Información Confidencial proporcionada por LA EMPRESA u obtenida por EL EMPLEADO durante sus labores a LA EMPRESA, o destruirlo en presencia de un representante autorizado por LA EMPRESA. Además, EL EMPLEADO certificará por escrito a LA EMPRESA la devolución y destrucción, según corresponda, de la Información Confidencial.
En caso de que EL EMPLEADO no cumpla con la devolución o destrucción según lo requerido en esta cláusula, se aplicará lo dispuesto en la cláusula séptima de este Acuerdo.

第 6 条
機密情報の返還と破棄
本契約が終了する場合、その理由に関わらず、「従業員」は、「会社」から提供された、または「会社」での勤務中に「従業員」が取得したすべての機密情報、そのすべてのコピー、および機密情報を含む機器、資料、書類などを返却すること、または、「会社」が承認する人の立会いのもと破棄することに同意する。また、必要がある場合は、「従業員」は、機密情報の返還および破棄を書面で会社に証明するものとする。
「従業員」が本条項で要求されている返却または破棄に従わない場合には、本契約の第 7 条の規定が適用される。

SÉPTIMA.
INCUMPLIMIENTO DEL ACUERDO

Cualquier incumplimiento de cualquier disposición del presente Acuerdo conllevará la obligación para EL EMPLEADO que cometió dicho incumplimiento, de pagar a LA EMPRESA una indemnización compensatoria por daños y perjuicios.

Asimismo, en caso de incumplimiento de la obligación de confidencialidad prevista en este Acuerdo, la relación laboral se dará por terminada sin responsabilidad alguna por parte de LA EMPRESA, de conformidad con la fracción IX del artículo 47 de la Ley Federal del Trabajo.

El incumplimiento de la obligación de confidencialidad prevista en este Acuerdo podrá constituir en un delito penal o podrá dar lugar a sanciones, quedando EL EMPLEADO sujeto a las sanciones que señalan la Ley Federal de Protección a la Propiedad Industrial, el Código Penal Federal y cualquier otra ley aplicable.

EL EMPLEADO reconoce que el incumplimiento de la obligación de confidencialidad establecida en este Acuerdo puede causar daños a las empresas involucradas. En cualquier caso, de incumplimiento de la obligación de confidencialidad, LA EMPRESA y/o cualquiera de las empresas con las que LA EMPRESA tenga la relación comercial tendrán los siguientes derechos:

a) Requerir y obtener una orden judicial de un Tribunal Competente para evitar que EL EMPLEADO incumpla o amenace con incumplir su obligación de confidencialidad;
b) Reclamar la reparación o denuncia penal ante el Fiscalía correspondiente para iniciar el procedimiento penal correspondiente; y
c) Exigir a EL EMPLEADO la reparación y el pago de los daños causados.

Cada vez que EL EMPLEADO incumpla o amenace con incumplir su obligación de confidencialidad, las empresas antes mencionadas tendrán los derechos antes descritos, incluso después de la terminación del presente Acuerdo.

第 7 条
契約違反

本契約のいずれかの規定に違反した場合、違反した「従業員」は、「会社」に対して損害賠償を支払わなければならない。

また、本契約に規定する機密保持義務が順守されない場合、「会社」は、連邦労働法第 47 条第 9 号の規定に従い、責任を負うことなく、雇用関係を終了させるものとする。

本契約に規定されている機密保持義務を遵守しない場合は、刑事犯罪となり、または罰が科される恐れがあり、「従業員」は、連邦産業財産権法、連邦刑法、その他適用され得る法の制裁の対象となり得る。

「従業員」は、本契約に定められた機密保持義務を遵守しない場合、関連する企業に損害が生じる可能性があることを確認する。どのような場合でも、機密保持義務に違反した場合、「会社」および「会社」と商業的関係のある企業は、次の権利を有するものとする。

a)「従業員」の機密保持義務違反や違反の恐れを止めるために管轄裁判所に裁判所命令を請求し取得すること

b) 対応する刑事手続きを開始するために、管轄となる検察に告訴すること

c)「従業員」に損失の回復と損害賠償を請求すること

「従業員が機密保持義務に違反した場合、または違反する恐れがある場合には、本契約の終了後であっても、前述の企業らはこれらの権利を有するものとする。

OCTAVA.

NO COMPETENCIA

EL EMPLEADO reconoce y se compromete a no competir con LA EMPRESA o cualquier otra empresa a la que LA EMPRESA preste servicios, directa o indirectamente y de cualquier forma, durante la relación laboral que exista entre LAS PARTES.

Asimismo, EL EMPLEADO no podrá realizar ningún negocio directamente con un socio, director, ejecutivo, empleado o consultor técnico, industrial o administrativo de personas naturales o jurídicas que LA EMPRESA preste servicios en relación con el servicio prestado por LA EMPRESA durante la relación laboral que exista entre LAS PARTES.

第 8 条

競業避止

「従業員」は、両当事者間に雇用関係がある間、直接的か間接的かを問わず、「会社」または「会社」がサービスを提供する他の企業と競合しないことを確認し、保証する。

また、「従業員」は、両当事者間に雇用関係がある期間中、「会社」の出資者、取締役、執行役員、従業員、技術・産業・経営コンサルタント、会社がサービスを提供する事業者と直接取引を行ってはならない。

NOVENA.

DIVISIBILIDAD

Cada cláusula de este Acuerdo pretenderá ser separable de las demás, de modo que, si alguna cláusula o término del mismo se considera ilegal o inválida por cualquier motivo, dicha ilegalidad o invalidez no afectará la validez de los términos y cláusulas restantes del mismo.

第 9 条

可分性

本契約の各条項は、他の条項から分離できるものであり、理由の如何を問わず、本契約の条項が違法または無効であるとみなされた場合には、かかる違法または無効性は本契約の他の条項に影響を与えないものとする。

DÉCIMA.
JURISDICCIÓN Y LEY APLICABLE

LAS PARTES reconocen estar vinculadas por el presente Acuerdo, así como por sus correspondientes anexos y modificaciones, en su caso, y sus efectos jurídicos y se comprometen a cumplirlo de buena fe.

Cualquier litigio relacionado, en especial, pero no sólo con la formación, validez, interpretación, suscripción, existencia, ejecución o terminación de este Acuerdo y, en general, con la relación establecida entre LAS PARTES se sujetará a las leyes de los Estados Unidos Mexicanos.

Para la interpretación y cumplimiento del presente Acuerdo, LAS PARTES acuerdan someterse a la jurisdicción y competencia de los Tribunales Federares, con renuncia expresa a cualquier otro fuero que por cualquier motivo pudiera corresponderles.

第 10 条
裁判管轄および適用法

両当事者は、本契約、該当する場合はその対応する付属書および修正条項、およびそれらの法的効果に拘束されることを認め、誠意を持ってこれに従うことを保証する。
特に、本契約の成立、有効性、解釈、合意、存在、履行または終了、および一般に当事者間で確立された関係に関連するすべての紛争は、メキシコ合衆国法に従うものとする。
本契約の解釈と遵守に関して、両当事者は、連邦裁判所の管轄権と権限に従うことに同意し、理由の如何を問わず、それに対応するその他の管轄権を明示的に放棄する。

DECIMO PRIMERO. (※)
IDIOMAS

Este Acuerdo se firmará tanto en español, como en [*idioma*], y todos los textos serán obligatorios y constituirán un mismo documento. En caso de contradicción, duda o discrepancia entre las versiones, prevalecerá la del idioma español.

第 11 条（※）
言語

本契約はスペイン語と(*言語*)の両方に署名され、全てが同じ文書を構成し、拘束力を持つ。両言語間に矛盾や疑義、相違がある場合は、スペイン語が優先される。

EN VIRTUD DE LO CUAL, LAS PARTES presentes han FIRMADO y ejecutado este Acuerdo en el día y año establecidos anteriormente.

以上より、両当事者は、冒頭に記載の日に本契約に署名しこれを締結した。

※契約書が 1 言語のみで作成される場合は不要

（ウ）退職後の協業避止条項（参考和訳付き）

●

No Competencia

En virtud del riesgo que afronta la Empresa, por el acceso a información privilegiada y/o confidencial, así como a secretos industriales y/o comerciales a los que el Trabajador tuvo acceso en virtud del puesto que desempeño dentro de la Empresa, El Trabajador se obliga, un plazo de [*duración*] contados a partir de la firma del presente Acuerdo, para proteger los intereses económicos y comerciales de la Empresa, a abstenerse totalmente de realizar las conductas que se enlista a continuación:

- Buscar con fines laborales a los empleados de la Empresa.
- Contactar a los proveedores de la Empresa.
- Contactar a los clientes de la Empresa.
- Contactar a los aliados comerciales de la Empresa.
- Divulgar por cualquier medio los secretos industriales o comerciales de la Empresa.
- Utilizar en beneficio propio o de un tercero los secretos industriales o comerciales de la Empresa.
- Utilizar la marca o signo distintivo de la Empresa sin su autorización.
- Trabajar para cualquier empresa competidora dentro del giro industrial.
- Fundar, constituir o iniciar una empresa que pudiera llegar a competir dentro del giro industrial.
- Asesorar o prestar servicios de consultoría en favor de cualquier empresa competidora dentro del giro industrial.
- Ser socio o accionista del órgano de administración de cualquier sociedad cuyo objeto social sea similar en actividades a las que realiza la Empresa.
- Lucrar de cualquier manera con información confidencial o privilegiada que pudiera implicar un perjuicio o la perdida de una ventaja para la Empresa.

第●条

競業避止

特権情報および/または機密情報、ならびに労働者が会社内での地位に基づいてアクセスできた産業秘密および/または商業秘密へのアクセスによる会社が直面する

リスクを考慮し、労働者は、会社の経済的および商業的利益を保護するために、本契約の署名から（*期間*）は、以下に挙げる行為を完全に行わないことを保証する。
・採用目的で会社の従業員に対し求人すること。
・会社のサプライヤーに連絡を取ること。
・会社の顧客に連絡を取ること。
・会社の商業提携先に連絡を取ること。
・いかなる手段によっても会社の産業上または商業上の秘密を開示すること。
・ 会社の産業上または商業上の秘密を自身または第三者の利益のために使用すること。
・会社の商標または独特の標識を許可なく使用すること。
・会社の産業分野の競合企業で働くこと
・産業分野で競合となるような会社を設立、創設、または起業すること。
・ 産業分野の競合企業に有利なアドバイスをしたり、コンサルティングサービスを提供したりすること。
・ 会社が実施する活動と企業目的が類似している企業の経営機関のメンバーとなるパートナーまたは株主となること。
・ 会社に損害を与えたり、会社が利益を失ったりする可能性のある機密情報や特権情報から何らかの形で利益を得ること。

●

Contraprestación a No Competencia

La Empresa se obliga a pagar en favor del Trabajador, por concepto de Contraprestación a cambio de su abstención de competir con la Empresa, la cantidad total de $[*Monto*] (*Monto a letras, -pesos 00/100 M.N.*), en una solo exhibición a la firma del presente acuerdo.

第●条(※)

競業避止への対価

会社は、労働者が会社との競争を放棄することの対価として、本契約に署名する際に、総額＄（*金額*）（*金額（文字）*）を一括で支払うものとする。

●

Incumplimiento a No Competencia（※）

Las Partes establecen que, para el caso de incumplimiento a clausula anterior denominada “No Competencia”,

i) el Trabajador se obliga a pagar en favor de la Empresa, por concepto de Pena Convencional la cantidad de $[Monto] (Monto a letras, -pesos 00/100 M.N.). o

ii) la Empresa podrá optar por exigir el pago de daños y perjuicios por dicho incumplimiento. En cuyo caso, la Empresa podrá optar por proceder judicialmente en contra del Trabajador y/o en contra de un tercero que haya sido beneficiado por el incumplimiento por parte del Trabajador, siempre y cuando dicho incumplimiento genere daños y/o perjuicios en detrimento de la Empresa.

En ese sentido, será la Empresa quien tendrá la facultad, en caso de incumplimiento, de optar por demandar el exigiendo el pago de la cantidad establecida como pena convencional u exigiendo el pago de daños y/o perjuicios por parte del Trabajador y/o un tercero beneficiado por el incumplimiento.

第●条
違反
両当事者は、前条「競業避止」違反があった場合には、次に従う。
i) 労働者は会社に対して違約金$（*金額*）（*金額（文字）*）を支払う。または
ii) 会社は、かかる不遵守に対して損害賠償の支払いを要求する。この場合、会社は、当該不遵守により会社に損害や損失が生じる場合に限り、当該労働者に対して、および/または労働者の不遵守により利益を得た第三者に対して、訴訟を起こすことを選択することができる。
この点に関し、会社は、違反があった場合に、違約金として定められた金額の支払いを求めるか、損害賠償や損失の支払いを労働者および/または違反によって利益を得ている第三者に求めるかを選択する権限を持つ。

退職時に退職合意書を作成することも多いため、退職合意書に記載することを前提として作成した。
※競業避止の対価を支払う場合を想定して作成していることから、これを支払わない場合は、変更が必要となる。

（エ）取引先との秘密保持契約（参考和訳付き）、取引先の管理体制チェックシート

●取引先との秘密保持契約

CONVENIO DE CONFIDENCIALIDAD CELEBRADO EL [*DD MM DE AAAA*], ENTRE [*Nombre de Empresa*], EN ADELANTE "LA EMPRESA", REPRESENTADA POR EL C. [*Nombre de Representante Legal*] Y [*Nombre de Empresa*], EN ADELANTE "******", REPRESENTADA POR EL C. [*Nombre de Representante Legal*], A QUIENES CONJUNTAMENTE SE LES DENOMINARÁ LAS "PARTES", Y QUE ESTÁN OBLIGADAS AL TENOR DE LAS SIGUIENTES DECLARACIONES Y CLÁUSULAS:

（法定代理人氏名）が法定代理人を務める(会社名)（以下、「会社」）と（法定代理人指名（会社名）（以下、「***」）（総じて「両当事者」）は、（年月日）に秘密保持契約を締結し、以下の各条項に拘束される。

DECLARACIONES

I. Declara EL EMPRESA, a través de su representante que:

1. Su representada es una sociedad constituida de acuerdo con las leyes de los Estados Unidos Mexicanos como consta en la escritura pública _____ de fecha ___ de _____ de _____, otorgada ante la fe del Notario Público número _____ _____, _____, la cual ha quedado debidamente inscrita en el Registro Público de la Propiedad y de Comercio de _____, bajo el folio mercantil electrónico número _____el __ de _____ de _____
2. El (Representante legal), se encuentra debidamente facultado para actuar en su representación y obligarlo en los términos de este Acuerdo, lo que acredita con copia de la escritura número _____ de fecha __ de _____ de _____, otorgada ante la fe del Notario Público número _____, facultades que hasta la fecha no le han sido revocadas, modificadas y/o limitadas en forma alguna.
3 Que señala como domicilio para todos los efectos derivados del presente Convenio el ubicado en calle _____.
3. Que está debidamente inscrita en el Registro Federal de Contribuyentes del Servicio de Administración Tributaria adscrito a la Secretaría de Hacienda y Crédito Público, con cédula de identificación fiscal _____.

II. Declara ***, a través de su representante que:

1. Su representada es una sociedad constituida de acuerdo con las leyes de los Estados Unidos Mexicanos como consta en la escritura pública _____ de fecha ___ de _____ de _____, otorgada ante la fe del Notario Público número _____ _____, _____, la cual ha quedado debidamente inscrita en el Registro Público de la Propiedad y de Comercio de _____, bajo el folio mercantil electrónico número _____el __ de _____ de _____
2. El [Representante legal], se encuentra debidamente facultado para actuar en su representación y obligarlo en los términos de este Acuerdo, lo que acredita con copia de la escritura número _____ de fecha __ de _____ de _____, otorgada ante la fe del Notario Público número _____, facultades que hasta la fecha no le han sido revocadas, modificadas y/o limitadas en forma alguna.

3. Que señala como domicilio para todos los efectos derivados del presente Convenio el ubicado en calle _____.
4. Que está debidamente inscrita en el Registro Federal de Contribuyentes del Servicio de Administración Tributaria adscrito a la Secretaría de Hacienda y Crédito Público, con cédula de identificación fiscal _____.

III. Declaran LAS PARTES conjuntamente, que:

1. Se reconocen mutuamente la personalidad con la que se ostentan a la celebración del presente Convenio.
2. Es su voluntad celebrar el presente Convenio con la finalidad de proteger la información confidencial propiedad de LAS PARTES que se lleguen a intercambiar con el objetivo de _____ (en lo sucesivo "el Propósito").

Con base en las anteriores declaraciones, LAS PARTES convienen en otorgar las siguientes:

宣言

I.「会社」は次のとおり宣言する

1. 「会社」は、公証人番号（番号），（氏名）によって証される、（年月日）付の公正証書（番号）に記載されているように、メキシコ合衆国の法律に従って設立された会社であり、（州）の商業登記簿に番号（番号）にて登録されている。
2. （法定代理人）には、「会社」に代わって行動し、本契約の条項に基づいて「会社」を拘束する権限が正式に、現在までにいかなる形でも取り消され、変更され、および/または制限されずに与えられており、公証人によって交付された、_____ 年 _____ 日付の証書番号 （番号）の写しを添付する。。
3. これは、本契約に基づくあらゆる目的において、（住所）にある住所を示す。
4. 大蔵公債省に付属する国税庁の連邦納税者登録簿に、納税者識別カード _____を以て正式に登録されている。

II.「***」は次のとおり宣言する

5. 「***」は、公証人番号（番号），（氏名）によって証される、（年月日）付の公正証書（番号）に記載されているように、メキシコ合衆国の法律に従って設立された会社であり、（州）の商業登記簿に番号（番号）にて登録されている。
6. （法定代理人）には、「会社」に代わって行動し、本契約の条項に基づいて「会社」を拘束する権限が正式に、現在までにいかなる形でも取り消され、変更され、および/または制限されずに与えられており、公証人によって交付された、_____ 年 _____ 日付の証書番号 （番号）の写しを添付する。。
7. これは、本契約に基づくあらゆる目的において、（住所）にある住所を示す。

8. 大蔵公債省に付属する国税庁の連邦納税者登録簿に、納税者識別カード _____を以て正式に登録されている。

III. 両当事者はともに次のことを宣言します。

1. 両者は、本契約を締結する人格を相互に認識します。

2. 両当事者は、その意思で（目的）する目的で本契約を締結する。

上記の宣言に基づいて、両当事者は以下を確認する。

CLÁUSULAS

条項

PRIMERA.

OBJETO DEL COMVENIO DE CONFIDENCIALIDAD

El objeto del presente Convenio es que LAS PARTES guarden estricta confidencialidad sobre la información propiedad de éstas, que se compartan entre sí ya sea de manera oral, escrita, por medios electrónicos, ópticos, electromagnéticos o por cualquier otro medio.

Se entenderá por Parte Receptora aquella que reciba “Información Confidencial” de la Parte Propietaria que será aquella dueña de la “Información Confidencial” entregada.

La Parte Receptora podrá utilizar la “Información Confidencial” única y exclusivamente para el propósito para el cual fue expresamente proporcionada y no podrá divulgarla ni utilizarla en forma alguna total o parcialmente, por sí o por interpósita persona, sin el consentimiento previo y por escrito de la Parte Propietaria de la información.

La información proporcionada con anterioridad a esta fecha, y que haya sido marcada como Confidencial, recibirá el mismo tratamiento a aquella información que se contenga bajo y con fecha posterior a la firma del presente.

Salvo en los casos expresamente establecidos en este Convenio, LAS PARTES se obligan a mantener rigurosamente en secreto y como confidencial la información de cada una de ellas, por lo que en ningún momento y bajo ninguna circunstancia podrán directa o indirectamente, divulgar, copiar, reproducir, alterar, revelar, o de cualquier otra manera hacerla del conocimiento de cualquier tercero en forma total o parcial, ni podrán explotar por sí o por interpósita persona, cualquier porción o la totalidad de la “Información Confidencial”.

No obstante, para los efectos de este Convenio, la Parte Receptora de la “Información Confidencial” estará exenta de guardar la confidencialidad respecto de aquella información que:

A) Haya sido puesta a disposición por un tercero, sin que esa divulgación quebrante o viole una obligación de confidencialidad de conformidad con este Convenio y las leyes aplicables de la materia.
B) Previamente a su divulgación fuese conocida por LAS PARTES, libre de cualquier obligación de mantenerla como Información Confidencial, según se evidencie por documentación que posea.
C) Sea o llegue a ser del dominio público o de carácter público con antelación o posterioridad a la celebración del presente Convenio sin mediar incumplimiento de este Convenio por alguna de LAS PARTES.
D) Haya sido desarrollada por cualquiera de LAS PARTES sin que dicha Parte haya tenido acceso a la Información Confidencial de la otra; y
E) Haya sido autorizada por la Parte Propietaria de la "Información Confidencial" para ser revelada, o que dicha Parte ya no la considere como "Información Confidencial" o privilegiada y así lo haya hecho saber.

Si a alguna de LAS PARTES se le solicitare o requiriere, por disposición de ley por parte de la autoridad judicial o administrativa competente a través de mandato escrito de conformidad con la legislación aplicable, como resultado de un procedimiento judicial o administrativo para revelar total o parcialmente la "Información Confidencial", la Parte que haya sido requerida conviene en informar inmediatamente a la Parte Propietaria de dicha información confidencial de tal requerimiento, lo anterior con la finalidad de que esta última tenga conocimiento de tal hecho, y si fuere el caso, esté en posibilidad de ejercer las medidas o recursos legales necesarios para una adecuada defensa si lo estima conveniente conforme a sus intereses.
Asimismo, la Parte Receptora se obliga a dar únicamente la "Información Confidencial" que le haya sido expresamente requerida por las autoridades judiciales o administrativas, haciendo su mejor esfuerzo para que en caso de que la autoridad no haya especificado el tipo de información requerida, realice el mejor método posible para afectar lo menos posible la obligación de no divulgar la "Información Confidencial". Para estos efectos la Parte que sea requerida para entregar la información deberá incluir en su respuesta la especificación de que la misma se encuentra protegida y clasificada como Confidencial en términos del presente Convenio.

第一条
本契約の目的
本契約の目的は、両当事者が、口頭、書面、電子的、光学的、電磁的、その他の手段を問わず、両当事者が所有する情報について厳格な機密を保持することである。

「受領者」は、引き渡された「機密情報」の所有者となる所有当事者から「機密情報」を受け取る者として理解される。
受領当事者は、明示的に提示された目的のためにのみ「機密情報」を使用することができ、所有当事者の事前の書面による同意がない限り、単独または仲介者を通じて、全体的または部分的にいかなる方法でも開示または使用することはできない。
本締結日より前に提供され、機密としてマークされている情報は、この文書に署名された後に扱われる情報と同じ扱いを受けるものとする。
本契約で明示的に定められている場合を除き、両当事者は、各当事者の情報を厳重に機密に保つことを約束し、いかなる時も、いかなる状況においても、直接的または間接的に、開示、複写、複製、改変、暴露することはできない。または、その他の方法で「機密情報」の全部または一部を第三者に開示したり、自らまたは仲介者を通じて利用したりすることはできない。
ただし、本契約の目的上、「機密情報」の受領者は、次の場合にその情報に関する機密保持義務を負わない。
A)本契約および関連法令に基づく機密保持義務に違反することなく、第三者によって提供されて場合
B)開示前に、それを機密情報として保持する義務がないことを当事者が認識しており、これが保有する文書によって証明される場合。
C)いずれの当事者も本契約に違反することなく、本契約の締結前または締結後にパブリックドメインまたは公共の性質を有することとなった場合。
D)いずれかの当事者によって、当該当事者が他方の機密情報にアクセスすることなく開発した場合
E)「機密情報」の開示を所有当事者によって許可されてた場合、または当該当事者がそれを「機密情報」または特権とみなさないとして、公表した場合
司法または行政手続きの結果として、管轄司法または行政当局により、適用法に基づく書面によって、「機密情報」の全部または一部を開示するよう要請または要求された場合、要請を受けた当事者は、当該秘密情報の所有当事者に当該要請を直ちに通知し、当該事実を当該秘密情報の所有当事者が認識し、必要に応じて適切な防御や必要な法的手段をとることができるようにすることに同意する。
同様に、受領当事者は、司法当局または行政当局から明示的に要求された「機密情報」のみを提供することを約束し、司法当局または行政当局が必要な情報の種類を指定していない場合には、「秘密情報」の不開示義務への影響を最小限に抑える最善の方法によって提供するよう努めるものとする。これらの目的のために、情報の提供を要求された当事者は、情報が保護され、本契約に従って機密として分類される旨の仕様を応答に含めるなければならない。

SEGUNDA.
INFORMACIÓN CONFIDENCIAL
Se entiende por “Información Confidencial” toda aquella información escrita, o gráfica en cualquier tipo de medio, así como la contenida en medios electrónicos o electromagnéticos, que se encuentre identificada claramente por LAS PARTES, sus filiales o subsidiarias como confidencial. Dentro de este tipo de información se incluye, de manera enunciativa más no limitativa, información técnica, financiera, crediticia y comercial relativa a nombres de clientes o socios potenciales, propuestas de negocios,

estrategias de negocios, estructura organizacional, estructura accionaria de las sociedades y de las partes integrantes de un grupo corporativo, los reportes, planes, proyecciones de mercado, datos y cualquier otra información industrial, económica o comercial, junto con fórmulas, mecanismos, patrones, métodos, técnicas, procesos de análisis, marcas registradas o no registradas, nombres o avisos comerciales, signos distintivos, patentes, obras intelectuales, documentos de trabajo, compilaciones, comparaciones, estudios o cualquier otro u otros documentos preparados, conservados e identificados con carácter confidencial por LAS PARTES, sus filiales o subsidiarias.

第 2 条
機密情報
「機密情報」とは、両当事者、その関連会社または子会社によって機密であると明確に識別されている、例えば電子媒体または電磁媒体といったあらゆる種類の媒体に含まれるすべての書面またはグラフィック情報を意味する。これには、技術情報、財務情報、信用情報、潜在的な顧客または出資者の名前、事業提案、事業戦略、組織構造、企業および企業の構成要素、企業グループ、レポート、計画、市場予測、データ、およびその他の産業、経済、商業情報、および式、メカニズム、パターン、方法、技術、分析プロセス、登録商標または未登録商標、名称または商業上の通知、独特の標識、特許、知的著作物、作業文書、編集物、比較、研究、または両当事者、その関連会社または子会社によって機密に基づいて作成、保存、特定されたその他の文書といった商業に関連する情報が含まれるが、これらに限定されない。

TERCERA.
CONFIDENCIALIDAD DE LA INFORMACIÓN
LAS PARTES reconocen que, para los efectos del presente Convenio la “Información Confidencial” constituye un secreto industrial en términos del artículo 163 de la Ley Federal de Protección a la Propiedad Industrial, y por lo tanto, quedará sujeta a lo establecido por los artículos 164, 165, 166, 167, 168 y 169 de dicho ordenamiento legal, por lo que la Parte Receptora podrá utilizarla única y exclusivamente para el propósito para el cual le fue expresamente proporcionada y no podrá divulgarla ni utilizarla en forma alguna sin autorización expresa y por escrito de la Parte Propietaria, el cual establece que para que los sujetos obligados.
LAS PARTES sólo podrán revelar la “Información Confidencial” que mutuamente se proporcionen, a sus empleados, accionistas, asesores, subcontratistas, representantes o cualquier persona que la requiera en forma justificada y únicamente para el Propósito para el cual la Parte Propietaria la haya entregado.
LAS PARTES harán que sus empleados, accionistas, asesores, subcontratistas, representantes que tengan acceso o conocimiento de la “Información Confidencial”, la guarden y mantengan bajo dicho carácter, cumpliendo con las obligaciones de

confidencialidad que aquí se estipulan. Lo anterior, en el entendido de que LAS PARTES deberán, en caso de ser necesario, celebrar todos aquellos contratos o convenios de confidencialidad a fin de que sus empleados, accionistas, asesores, subcontratistas, representantes o cualquier persona que la requiera justificadamente protejan la "Información Confidencial".

Asimismo, cada una de LAS PARTES deberá capacitar a sus empleados, accionistas, asesores, subcontratistas, representantes con relación al uso y cuidado que deben guardar respecto de la "Información Confidencial", así como darles a conocer los alcances de las obligaciones de confidencialidad contenidas en el presente documento.

LAS PARTES deberán proteger la "Información Confidencial" que les haya sido revelada, con el mismo grado de cuidado, pero nunca en grado menor al que emplean para proteger su propia Información Confidencial.

第 3 条
機密性

両当事者は、本契約の目的上、「機密情報」は連邦産業財産権保護法第 163 条の観点から産業秘密を構成し、したがって第 164 条、第 165 条、第 166 条、第 167 条、第 168 条および第 169 条の規定が適用されるため、受領当事者は、明示的に提供された目的のためにのみにそれを使用することができ、所有当事者の書面による明示的な許可がない限り、いかなる方法でも開示または使用することはできない。

両当事者は、相互に開示する「機密情報」を、正当な方法で、所有当事者が提供した目的のためにのみ、従業員、株主、アドバイザー、下請け業者、代理人、またはそれを正当な事由を以て必要とする人物にのみ開示することができる。

両当事者は、「機密情報」にアクセスできる、またはこれを知る従業員、株主、アドバイザー、下請け業者、代理人が、本契約に規定されている機密保持義務を遵守し、機密情報を保存および保持することを保証します。これは、両当事者が必要に応じて、従業員、株主、アドバイザー、下請け業者、代理人、または正当に知る必要のある人物が「機密情報」を保護できるように、これらすべてと機密保持契約を締結しなければならないことを理解した上で行うことができる。

また、各当事者は、従業員、株主、アドバイザー、下請け業者、代理人に対し、「機密情報」の使用や保持について研修を行うとともに、本契約に規定される守秘義務の範囲を周知させ、「機密情報」関する遵守事項を遵守させなければならない

両当事者は、開示された「機密情報」を、自らの機密情報を保護する場合と同程度またはそれ以上の注意をもって、保護しなければならない。

CUARTA.
PROPIEDAD DE LA INFORMACIÓN

LAS PARTES reconocen que la "Información Confidencial" que manejen entre ellas es propiedad exclusiva de la Parte Propietaria que la otorgue.

Asimismo, la celebración del presente Convenio no le confiere a ninguna de ellas respecto de la “Información Confidencial” de su contraparte, derechos., autorizaciones, permisos, o licencias de propiedad industrial o intelectual, sobre la misma.
Ninguna de LAS PARTES podrá elaborar copias de la “Información Confidencial” sin el previo consentimiento por escrito de la Parte Propietaria de la información.

第 4 条
情報の所有権
両当事者は、両当事者間で管理する「機密情報」が、それを開示する所有当事者の独占的財産であることを確認する。
同様に、本契約の締結は、相手方の「機密情報」に関する権利、認可、許可、工業所有権または知的財産権のライセンスのいずれをも付与するものではない。
いずれの当事者も、情報の所有当事者の事前の書面による同意がない限り、「機密情報」の複写を作成することはできない。

QUINTA.
DEVOLUCIÓN DE INFORMACIÓN CONFIDENCIAL
La Parte Propietaria de la “Información Confidencial” tendrá el derecho de exigir en cualquier momento a la Parte Receptora que dicha información sea destruida o devuelta, independientemente de que la misma se haya entregado o revelado antes o después de la celebración de este Convenio, en el entendido de que dicha destrucción o devolución no terminará con las obligaciones de confidencialidad señaladas en este Convenio.

第 5 条
機密情報の返還
「機密情報」の所有当事者は、本契約締結の前後に提供または開示されたかどうかに関係なく、いつでも受領当事者に対し、当該情報の破棄または返却を要求する権利を有する。当該破棄または返却によって、本契約に示されている機密保持義務が終了するものではない。

SEXTA.
TERMINACIÓN DE LA RELACIÓN CONTRACTUAL
En caso de que LAS PARTES den por terminadas sus relaciones de negocios o contractuales, sin importar la causa de dicha terminación, no las exime de cumplir todas las obligaciones a su cargo establecidas en el presente Convenio.

第 6 条
契約関係の終了

両当事者がビジネスまたは契約関係を終了する場合、その終了の原因を問わず、本契約で定められたすべての義務の遵守が免除されるものと解されてはならない。

SÉPTIMA.
DAÑOS Y PERJUICIOS

Para el caso de que la Parte, incluyendo a sus respectivos empleados, filiales, agentes, asesores, representantes o cualquier persona que requiera en forma justificada la "Información Confidencial", incumplan o violen alguna de las estipulaciones del presente Convenio, pagará a la otra Parte, los daños y perjuicios debidamente probados que tal incumplimiento le ocasionen, en el entendido además que este último quedará facultado para ejercitar todas las acciones civiles o penales como en derecho mexicano proceda en contra de la Parte por haber divulgado la información.

第 7 条
損害

当事者（それぞれの従業員、子会社、代理人、アドバイザー、代表者、または「機密情報」を正当に必要とする人物を含む）が本契約の規定のいずれかを遵守せず、または違反した場合、これに基づき生じる損害について当事者は相手方当事者に賠償金を支払うものとする。また、情報を開示した当事者に対してメキシコの法律に基づく適用可能なすべての民事または刑事訴訟を行使することができる。

OCTAVA.
NO CESIÓN

Sin excepción, ninguna de LAS PARTES podrá ceder los derechos y obligaciones que este Convenio le impone sin previo consentimiento por escrito de la otra Parte, el cual deberá constar en convenio escrito debidamente firmado por ambas partes, en el entendido que, cualquier cesión pretendida o realizada que no cumpla con este requisito, será nula.

第 8 条
譲渡の禁止

例外なく、両当事者は、相手方当事者の事前の書面による同意なしに、本契約に課せられる権利と義務を譲渡することはできない。この要件を満たさない譲渡は無効となり、要件を満たす譲渡の場合は、両当事者が正式に署名した契約書を作成し記録する。

NOVENA.
VIGENCIA

El presente Convenio entrará en vigor a partir de la fecha de su firma y permanecerá vigente por un periodo de ___ (_____) años contados a partir de dicha fecha.

Al término del Convenio, LAS PARTES seguirán obligadas a no divulgar o usar la "Información Confidencial" por un periodo de tres (3) años a partir de la fecha de terminación y a devolverse de inmediato todos los documentos y materiales de su propiedad que contengan "Información Confidencial" que con motivo de la celebración y ejecución del Convenio haya sido comunicada o entregada, así como a destruir cualquier copia de sus archivos electrónicos o de cualquier otra naturaleza que mantenga

第 9 条
期間
本契約は署名日から発効し、当該日から●年間有効となる。
本契約終了後も、両当事者は、終了日から 3 年間は「機密情報」を開示または使用しない義務を引き続き負うものとし、両当事者は、本契約の締結および実行のために開示等を受けた自身が所有する文書および資料を直ちに返却し、また、その電子ファイルまたはその他の方法による複写を破壊する義務を負う。

DÉCIMA.
MODIFICACIONES
LAS PARTES acuerdan que ninguna modificación al presente Convenio será válida o tendrá efecto legal alguno a menos que conste por escrito mediante convenio modificatorio debidamente firmado por ambas partes especificando la naturaleza de dichas modificaciones.

第 10 条
変更
本契約の変更は、当該変更の内容を明記し両当事者が正式に署名した変更契約の形で書面に記録されなければならず、それ以外の方法による本契約の変更は無効であり、法的効果もない。

DECIMO PRIMERO.
AVISOS Y NOTIFICACIONES
Todas las notificaciones requeridas o permitidas bajo este Convenio deberán ser entregadas por escrito o vía electrónica y de manera indubitable, en los siguientes domicilios o direcciones de correo electrónico. Dichas notificaciones surtirán efectos cuando sean efectivamente recibidas por el destinatario o su representante:

LA EMPRESA
_____
_____
_____

＊＊＊

_____
_____
_____

En caso de que cualquiera de LAS PARTES cambie de domicilio o de dirección de correo electrónico, se obliga a avisar a la otra Parte con al menos 15 (quince) días hábiles de anticipación a la fecha efectiva del cambio, mediante documento escrito debiendo obtener el acuse de recibo correspondiente.

第 11 条（※）

通知

契約に基づいて要求または許可されるすべての通知は、書面または電子的かつ明確な方法で、次の住所または電子メール アドレスに送信するものとする。上記の通知は、受信者またはその代理人が実際に受信したときに発効する。

LA EMPRESA

_____
_____
_____

＊＊＊

_____
_____
_____

いずれかの当事者が住所または電子メール アドレスを変更する場合、変更発効日の少なくとも 15 営業日前までに書面で他方当事者に通知する義務があり、また、その受領確認を取得しなければならない。

DECIMO SEGUNDO.

LEGISLACIÓN Y JURISDICCIÓN APLICABLE

Para la interpretación y cumplimiento del presente Convenio, LAS PARTES se someten expresamente a las leyes y los tribunales competentes de la ［Ciudad de México］, renunciando a cualquier otro fuero que pudiere corresponderles por razón de sus domicilios presentes o futuros.

El otorgamiento y la ejecución del presente Convenio, el intercambio de “Información Confidencial” y cualquier actuación de LAS PARTES al amparo del mismo no constituirá ni supondrá, en ningún caso, promesa, intención o compromiso de cualquiera de LAS PARTES de adquirir ningún producto o servicio de la otra,

comercializar o vender bienes o servicios de la otra Parte (ahora o en el futuro); distribuir o proveer cualquier producto o servicio; o de cualquier manera contratar o alcanzar cualquier tipo de transacción o acuerdo con la otra Parte.

第 12 条
準拠法と裁判管轄
本契約の解釈と遵守に関して、両当事者は明示的に（メキシコシティ）の法律および管轄裁判所に服従し、現在または将来の住所を理由に該当可能性のあるその他の裁判管轄を放棄する。
本契約の締結および履行、「機密情報」の交換、およびこれに基づく両当事者の行為は、いかなる場合においても、製品の購入、相手方のサービス、相手方の商品またはサービスのマーケティングまたは販売（現在または将来）、製品またはサービスの流通または卸売、または、何らかの方法で相手方当事者と契約するか、あらゆる種類の取引または合意に達することという両当事者の約束、意図、約束を構成または暗示するものではない。

Leído que fue el presente convenio por LAS PARTES y debidamente enteradas de su contenido y alcance legal, lo suscriben de conformidad y por duplicado, en la （Ciudad de México）.

両当事者は、この契約を読み、その内容と法的範囲を正式に確認したのち、（メキシコシティ）において、本書 2 通に署名した。

●取引先の管理体制チェックシート

Categoría	Ítem	Evaluación
Política y sistema de gestión	Establecer una persona responsable y un departamento encargado de la gestión de la información.	
	Formular normas o manuales de gestión de secretos comerciales.	
	Dichas reglas o manuales se deberán revisar oportunamente y actualizarse según corresponda.	
Identificación de secreto	Elaborar una lista de la información retenida que esté sujeta a confidencialidad, y en ella se incluirá la información divulgada por (***).	
	La información será clasificada y la información confidencial, incluída la de (***), se deberá identificar.	
	Determinar autorizaciones de acceso en función de la importancia del secreto.	
	Controlar la entrada y salida de personas ajenas.	

Manejo físico	Cuando entren personas ajenas, deberán llevar insignias para poder ser reconocidos como personas externas.	
	Limitar las áreas a las que pueden ingresar personas externas, así como separar la sala de reuniones y las áreas de oficina.	
	Los medios de grabación confidenciales deberán estar etiquetados como "Confidencialidad".	
	Gestionar de forma separada la información general. Los papeles, etc. se mantendrán bloqueados.	
	Poder consultar los registros de uso de la impresora.	
	Tomar medidas para restringir las copias.	
	Mantener registros de los artículos retirados y devueltos.	
	Tomar medidas para evitar robos al sacar artículos.	
	El sitio de producción/fabricación estará debidamente dividido para que personas ajenas no puedan verlo.	
	El uso de teléfonos celulares estará prohibido o restringido dentro de los sitios de producción y fabricación. O bien, el número de trabajadores disponibles estará limitado.	
	El acceso a áreas que manejen información confidencial sensible estará restringido.	
	Las áreas de acceso restringido se gestionarán adecuadamente, por ejemplo, manteniendo registros de entrada y salida.	
	Se instalarán cámaras de vigilancia en áreas que contengan información confidencial de gran importancia.	
Manejo técnico	Los datos electrónicos conservados se gestionarán en un servidor y se elaborarán registros de acceso.	
	Se tomarán medidas de protección contra el acceso externo a las PC que administren información confidencial.	
	Establecer una contraseña en la computadora del trabajador.	
	Las contraseñas de la computadora se deberán cambiar periódicamente.	
	Se gestionarán las computadoras que estén fuera de la empresa.	
	Prohibir o restringir las conexiones de las computadoras a redes públicas.	
	Prohibir o restringir el uso de aplicaciones de comunicación.	
	El uso de medios de almacenamiento personales como USB estará prohibido o restringido.	

	Los administradores estarán identificados y los derechos de acceso se limitarán según el grado de confidencialidad.	
	Poder consultar el historial de envío de correos electrónicos y el historial de navegación en sitios web.	
	La existencia de métodos exhaustivos de eliminación para garantizar que la información no podrá leerse después de utilizar las copias.	
Gestión Humana	Brindar capacitación al ingresar a la empresa y periódicamente en lo posterior para crear conciencia sobre la importancia de proteger los secretos comerciales.	
	Celebrar acuerdos de confidencialidad sobre secretos comerciales (Las disposiciones se establecerán en el contrato de trabajo).	
	Especificar información que está clasificada como confidencial.	
	Gestionar la devolución y eliminación de información confidencial divulgada.	

参考和訳

カテゴリー	チェック項目	評価
管理方針・体制	情報管理責任者、情報管理担当部署等を設けている。	
	営業秘密管理規定や管理マニュアルが策定されている。	
	規定やマニュアルは、適宜更新されている。	
秘密の特定	秘密保持の対象となるような保有情報をリスト化している。（＊＊＊）から開示された情報がそのリストに含まれている。	
	保有情報の区分をし、（＊＊＊）の情報を含め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限者を決めている。	
物理的管理	外部者の入退出管理を行っている。	
	外部者が立ち入る際には、外部者と認識できるようバッジ等をつけている。	
	ミーティングルームと執務室のエリアを分けるなど、部外者が立ち入ることのできるエリアを限定している。	
	記録媒体に「Confidencialidad」など秘密であることの表示がされている。	
	一般情報と区別し、管理されている。紙媒体等を施錠管理している。	
	プリンターの利用記録が確認できる。	
	複製を制限する措置がとられている。	
	持ち出しや返却の記録が作成されている。	
	持ち出しの際の盗難防止対策がとられている。	

	生産・製作現場の様子が外部者に見えないよう適切に仕切られている。	
	生産・製作現場内では携帯電話の使用が禁止・制限されている。もしくは、使用できる労働者が限定されている。	
	重要度の高い秘密情報を取り扱うエリアへのアクセスを制限している。	
	アクセス制限エリアについて、入退室記録をとるなど、適切に管理している。	
	重要度の高い秘密情報があるエリアには監視カメラを設置している。	
技術的管理	保有する電子データをサーバー上で管理し、アクセスログを記録している。	
	秘密情報を管理する PC に外部からのアクセスに対する防護策をとっている。	
	労働者の PC にパスワードが設定されている。	
	PC のパスワードは定期的に変更されている。	
	PC の社外持ち出しを管理している。	
	PC の公共ネットワークへの接続を禁止・制限している。	
	コミュニケーションアプリの使用を禁止・制限している。	
	私物の USB 等の記録媒体の使用を禁止・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。	
	メール送信記録やウェブサイトの閲覧履歴を確認できる。	
	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	入社時やその後も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。	
	営業秘密に関し秘密保持契約を締結している（雇用契約書に規定を設けている。）	
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。	
	開示した秘密情報の返還や廃棄を管理している。	

（オ）来訪者受付表（秘密保持への同意）

REGISTRO DE VISITANTES.

Fecha	Visitante		Destino		Hora		Firma
	Nombre	Empresa	Departamento	Persona	Entrada	Salida	

Para visitar el establecimiento de *** (***), acepto las siguientes prohibiciones y reconozco las consecuencias legales que su incumplimiento contrae:

1. Tengo prohibido tomar fotografías, películas o registros de vicio/sonido en su establecimiento sin el consentimiento previo de (***).
2. Tengo prohibido revelar la información que vi y conocí mientras visitaba el establecimiento de (***).
3. Cuando (***) sufra daños por mi incumplimiento de lo anterior, (***) podrá reclamar el daño conforme a lo dispuesto en las leyes y reglamentos aplicables.

Nombre de Empresa　　Fecha, Nombre y Firma

参考和訳

訪問者登録

日付	訪問先		訪問先		時間		署名
	氏名	会社名	部署	名前	入館	退館	

*** (以下、***)の施設を訪問するにあたり、以下の禁止事項を認め、遵守しない場合に生じる法的影響を確認する。

1. (***)の事前の同意なく、貴施設内で写真、映画の撮影、音声の記録は禁止される。
2. (***)の施設を訪れた際に見聞きした情報を公開することは禁止される。
3. 私が上記の遵守を怠ったことにより（***）に損害が生じた場合、(***）は法令の規定に従い損害賠償を請求することができる。

会社名　　日付、氏名、署名

（カ）メキシコを対象とした関連あるガイドライン等

メキシコを対象とした営業秘密に係るガイドラインは見つけられなかった。

---

[i] 特許庁　諸外国・地域・機関の制度概要および法令条約等「メキシコ」より（以下、法の日本語翻訳について同じ。）
https://www.jpo.go.jp/system/laws/gaikoku/document/mokuji/mexico-sangyou.pdf
(2023 年 12 月 15 日最終アクセス)

[ii] 特許庁　諸外国の法令・条約等　TRIPS 協定より
https://www.jpo.go.jp/system/laws/gaikoku/trips/chap3.html#anchor7setu　(2023 年 12 月 15 日最終アクセス)

[iii] Meta Platforms, Inc.関連会社が提供するコミュニケーションサービス

[iv] https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf　(2023 年 12 月 15 日最終アクセス)

[v] Suprema Corte de Justicia de la Nación, Amparo directo 406/2011
https://sjf2.scjn.gob.mx/detalle/tesis/2003833　(2023 年 12 月 15 日最終アクセス)

[vi] https://camex.com.mx/arancel-y-calculador/　(2023 年 12 月 15 日最終アクセス)

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］
TNY LEGAL MEXICO S.A. DE C.V.
独立行政法人 日本貿易振興機構 メキシコ事務所
2024年３月

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。

経済産業省委託事業

中国における営業秘密管理マニュアル

2024 年 3 月

独立行政法人　日本貿易振興機構

上海事務所

はじめに―増補・改訂版によせて

「中国における営業秘密管理マニュアル」の初版のリリースは 2020 年です。その後、関連する司法解釈等において、いくつか重要な改正がありましたので、今回、本マニュアルの改訂を行うことになりました。マニュアルの柱となる第 3 章の「漏えい対策実践編」の 1 ～ 4 の事前の予防措置の主なポイントは、法改正によって変わるものではなく、初版から大きな変更はありませんが、今回の改訂・増補版では、取り上げる裁判例やトピックをアップデートするとともに、特に、中小企業にとっても分かりやすく、実践的な内容とすることに主眼において、構成を変更、また、例えば、参考書式に携帯電話、SNS 管理規定を追加する等、初版の内容に全体的に加筆しています。

2022 年、平和と安全、経済的な繁栄等の国益を経済上の措置を通じて確保することを目的とした経済安全保障推進法が成立しました。国益を支える技術や情報財を保護するための知的財産関連政策、法制は極めて重要であり、同法の制定には、中国などを含む諸外国との関係性を念頭に置いた、日本企業の知的財産保護の必要性が一層高まっていたことが、その背景の 1 つとして挙げられるところです。ここで、改めて、経済的な側面からの「国益」とは何かを考えてみると、それは、規模の大小を問わず、経済体としてのわが国を構成する企業一社一社により積み上げられた経済的利益の総体にほかならないのですから、真の意味で国益を確保するには、各社の技術や情報財が知的財産として、国内外を問わず、適切に保護されるようにすることが不可欠であると考えられます。もっとも、中国拠点における知的財産の保護は、基本的には、中国の法制度の枠内での問題となるので、日本国内の法整備による対応にはもとより限界があり、中国で事業を行う日本企業は、「自社の営業秘密は自社で守る」という意識を持って対策を考える必要があります。

こと中国に関しては、わが国との社会システムの相違や、それに関する日本国内での報道に日々触れる中で、どうしても、一企業では対策のしようがないという認識を与えてしまいがちです。しかし、実際に中国で発生している知的財産侵害の大多数は、むしろ「足元」で発生していること―すなわち、現地従業員が金銭目的で営業秘密を競合企業に漏えいする、あるいは、幹部社員が競合会社を自ら立ち上げてそこで営業秘密を流用する、というパターンが圧倒的に多いとい

う事実を、まず理解する必要があります。そして、こうしたケースは、振り返れば、事前の予防法務的措置を講じておくことで、未然に防ぐことができたのではないかと思われることが多いのです。本マニュアルは、このような観点から、中国における営業秘密侵害の実態を踏まえ、中国法とそのプラクティスに基づき、各社自ら、中国拠点における営業秘密管理体制を整備することができるよう、管理の手法と社内での体制構築の進め方を具体的に説明しています。

日本の技術の素晴らしさは、大企業・中小企業を問わず、世界的にも、長年、高く評価されているところであり、そのために、中国を含む海外において、模倣・盗用の対象として狙われやすい傾向にあります。日本の技術が、中国をはじめ、社会的慣習も人々の考え方も大きく異なる国々においても適切に保護されるべく、本マニュアルが、中国における営業秘密管理の強化を目指し、まずは「足元」から管理体制の見直しを図ろうとする各企業の力となれば幸いです。

目次

本マニュアルの使い方

筆者が中国における日系企業の営業秘密体制の構築支援に携わる中で、日系企業の管理体制構築状況は大きく以下の２パターンに分かれていました。

①「ほぼ手つかず」状態
漠然とした危機感を持ちながらも、具体的に何をやっていいかが分からず、中国拠点における営業秘密管理体制の構築が手つかずのままとなっている。
②ある程度、体制構築が進んでいる状態
日本本社の営業秘密管理体制を横展開等する形で、ある程度の管理体制は構築できている。

①の場合、まずは、
・第Ⅰ章の全部
を読み、中国で実際に起きていることを理解して頂いた上で、「自分ごと」として取り組む意識を持って頂きたいと思います。
そして、第Ⅲ章で説明する採るべき各対策の理由や位置づけを理解するために、やや抽象的な法律論にはなりますが、
・第Ⅱ章の１と２
も、あわせて読んでみて下さい。
その上で、
・第Ⅲ章
を参考に、実際に取り組みを始めて頂きたいと思います。

①の場合、企業によっては、管理体制を構築する前から、「中国で対策をしても無駄ではないか？」と対策をとること自体に懐疑的であるケースも散見されます。しかし、何らの措置も講じていないと、実際に漏えいが発生した時に、法的な救済を受ける可能性を自らゼロにしてしまうことになります（その理由は第Ⅱ章の１で説明します）。また、第Ⅰ章で紹介するような、ショート動

画を通じた営業秘密の漏えいが疑われる事案では、投稿者（従業員である可能性が高い）の悪意は感じられず、従業員への周知・教育を含めた SNS 使用に対する対策が講じられていれば、このような事態を防げたのではないかとも思われます。
第Ⅲ章で説明する管理体制の構築は、各企業において、保護すべき営業秘密の内容・形態や、人員体制などによって異なってくるため、①の状態の場合、特に第Ⅲ章のステップ 2 以降の対応が自社では難しい場合もあるかもしれません。そうした場合には、法律・技術の専門家に相談するなど、外部の力を借りることも一案です。例えば、執筆時点で、在中国の日系企業を対象に、そのような専門家のアドバイスを無償で受けられる、JETRO の支援事業もあります。

一方、②は、中国での営業秘密漏えいリスクは既に十分に理解しており、かつ、基本的な管理体制の構築は行ってきている状態といえます。このような企業からは、リスクを完全にゼロにする完璧な手段を教えてほしいと求められることが多いです。しかし、残念ながら、リスクを完全にゼロにできる絶対解があるわけではありません。営業秘密の漏えい防止に限らず、およそリスクマネジメントとは、多角的に－つまり複数の角度から幅広く、そして、階層的に－つまりより深く、様々な対策の積み重ねによって、より強固になっていく性質のものです。したがって、ある程度、体制構築が進んでいる企業の場合、中国での営業秘密管理を考える上での重点ポイントの優先的な見直しを行いつつ、トータルで対策の「穴」を埋めていくことをお勧めします。その「穴」を埋めるためには、まずは、「穴」を見つけなければなりません。そのための手段として有効なのが、第Ⅲ章で説明する「セルフチェックシート」です。
そこで、②の状態の場合には、
・第Ⅰ章の 1
を読み、中国での営業秘密を考える上での重要ポイントを把握した上で、
早速、
・第Ⅲ章の 2 のステップ 1 のセルフチェックシート
を用いて、自社の対策に「穴」がないかを確認の上、第Ⅲ章を参考に重点的な対策を検討してみて下さい。
なお、セルフチェックシートには項目がないのですが、②のパターンでは、ある程度体制ができているがゆえの盲点－社内規定が法改正に対応できていな

い―などがよく見受けられます。法制度について説明している第 II 章も、あわせて確認して頂くのが望ましいと思います。

第Ⅰ章（基礎知識編）

本章のポイント

- 中国では近年、ショート動画 SNS や、中国最大のチャットアプリである WeChat を通じた営業秘密漏えい事案が目立っており、対策が急務である。
- 日系企業の間でも、従来から、中国現地法人社員による営業秘密侵害の被害が発生しており、その被害はいずれも深刻である。
- 漏えいパターンとしては、従業員から漏えいするパターン、取引先から漏えいするパターン、第三者が不正に取得するパターンに分けることができるが、この中でも従業員から漏えいするパターンが従来から大きく問題となっている。

１．中国における営業秘密侵害の実態―今、中国で何が起きているのか

（１）ショート動画 SNS を通じた営業秘密漏えい

ここ数年、ショート動画 SNS「Tik Tok」は、日本でも若者を中心に人気を集めています。この TikTok が、2023 年 2 月、米国において、中国政府にユーザ情報が流出している可能性があることを理由に、連邦政府職員の公用端末での使用が禁止されたことは日本でも広く報道され、記憶に新しいところです。

しかし、中国ではすでに、その数年ほど前から、ユーザ数 8 億人を超えると言われる「抖音」（Douyin 中国版“TikTok”）をはじめとするショート動画 SNS[1]を通じた、企業の営業秘密漏えいが問題視されており、筆者も実際に、ある日系企業の中国工場内で撮影されたことが疑われる動画を目にしたことが何度かあります。こうした個人の投稿動画には、投稿時に工場位置が付加されており、位置情報から容易に、どの工場で撮影された動画なのかを知ることができるものが含まれ、中には、タイトルやキャプションに工場名が明記された動画もありました。また、こうした動画は、個人のスマートフォンで撮影されたと思われますが、近

[1] ほかに、「快手（Kuaishou）」や「微視（We Show）」など。

年のカメラ機能の向上により、機械の詳細な動作や作業工程を記載したと思われる掲示内容がかなり鮮明に映っていたものもありました。

参考：Douyin サイト（https://www.douyin.com/）

おそらくそのような動画は、探せば簡単に見つけることができると思います。このように、ここ数年で、「抖音」をはじめとするショート動画 SNS を通じた、工場内を撮影した動画の流出事例が目立ってきています。そして、その多くは、公開動画を見る限り、当該工場で働く従業員が、私物のスマートフォンで撮影した動画をアップロードしていると思われるものです。工場内で撮影された動画に必ずしも営業秘密情報が含まれるとは限らないですが、工程表まで映り込む場合も実際にあり、その線引きは困難であることに加えて、このような動画が流出すること自体、自社の情報管理体制に問題があると考えなければなりません。

（2）国家機関も警鐘を鳴らす“微信”（We Chat）

1 で挙げた「抖音」はショート動画に特化した SNS アプリですが、登録ユーザ数が 10 億人を優に超える中国最大のチャット SNS アプリである「微信」（We Chat）を通じた営業秘密の漏えいも引き続き問題となっています。

国務院が主管する、中国全土の秘密保持業務の職責を担う「国家保密局」では、「くれぐれも微信（WeChat）を秘密に係る業務に使用してはならない」と題する、漏えい事例を紹介した記事[2]が 2018 年に公表されています。このほかにも、同局は 2022 年、微信が秘密漏えいの「被災地」であると指摘した記事を宣伝教育ページ[3]で紹介するなど、微信の業務上の利用に注意するよう呼びかけを行っ

[2] http://www.gjbmj.gov.cn/n1/2018/0605/c409095-30037166.html

[3] http://www.gjbmj.gov.cn/n1/2022/0913/c409092-32524897.html

ています。このように、国家機関が微信を通じた情報漏えいについて繰り返し警鐘を鳴らすほど、中国では微信を通じた情報漏えいが問題となっているということです。

微信を通じた情報漏えいのパターンとして良く見受けられるのが、

①「朋友圏（日本語版では「モーメンツ」）」というタイムライン投稿欄に、「抖音」と同様のショート動画等の形式で秘密情報を公開する、

②社内のグループチャットで共有するファイルを他のユーザに誤送信する、

というものです。

②の漏えいが発生する背景として、中国では、業務上のやり取りにこの微信が非常によく使われていること、また、①の漏えいと共通の背景として、私物のカメラ付き携帯電話（スマートフォン）が業務時間内に普通に使われている、ということが挙げられます。

以上のように、中国では、近年、SNS アプリの利用により、インターネットを通じて、即時にかつ広範に、営業秘密が流出する事例が多発しており、中国において営業秘密を保護するためには、SNS 規制と、その手前の携帯電話（スマートフォン）規制を考えることが必須となることが分かります。

2．なぜ、営業秘密を保護する必要があるのか

では、なぜ、営業秘密を保護する必要があるのでしょうか。ここでは、実際に中国で営業秘密侵害の被害に遭った日系企業の例を 2 つ挙げて説明します。

（1）化学系メーカの事例[4]

日系企業 A 社は 、2004 年に昆明市に工場を設立し、同年、後に A 社の営業秘密を盗用することになる中国人職員 B を採用しました。A 社の社長は、B の真面目で研究熱心な姿勢を評価し、同社の主力商品であり、健康食品等に用いられる色素成分、アスタキサンチンの製造技術をたたき込んだということです。ところが、その 5 年後、B は A 社を退社。

[4] https://www.sankei.com/article/20150409-IYJDOJ52JJICDCHR5FR5UIQ32A/

その翌年、A 社中国工場と同じく「アスタキサンチン」を製造する C 社が、A 社の開発技術について、4 件の実用新案権を取得していることが発覚しました。A 社は、この実用新案権を取り戻すべく B らを提訴し、勝訴判決を得ましたが、当該実用新案は B らが登録料を滞納し、その後適切な手続きがされなかったため、A 社の権利として取り戻すことができませんでした。すなわち、A 社が何年もかけて開発した技術が、B らの冒認出願によって勝手に公開されてしまい、しかも、権利の消滅により誰でも自由に実施できる技術となってしまったのです。

この事件による A 社の被害額は十数億円規模にも上るといいます。

（2）電機メーカの事例[5]

日系企業 D 社は、2001 年に広州市に工場を設立し、水銀ランプなどの製品を生産しています。同工場の製造部、品質部の管理職である E は、2005 年から 2012 年にわたり、水銀ランプの製造技術を不正に取得した上、2015 年に D 社を退職して F 社を設立し、そこで水銀ランプの生産を開始しました。本件は刑事事件として起訴され、E は懲役 5 年、罰金 500 万元の刑に処されました。しかし、F 社による営業秘密侵害品の製造販売は約 5 年にもわたり、監査の結果明らかとなった F 社の 3 年間の水銀ランプの粗利益は 7,400 万元余りに及んだということです。

以上のように、製造技術などの営業秘密が侵害されると、自社製品と類似の模倣品が流通することになります。模倣品は研究開発コストを製品に上乗せする必要がない分、正規品よりも相当安価で販売されることが多く、**価格が重視される中国では、権利者の製品は、大抵、売り負けてしまう**のです。つまり、営業秘密侵害は、自社製品の売上げの大幅な減少につながるということです。しかも、これらの事例のように、盗用された営業秘密が自社の主力製品の製造技術である場合には、その被害は計り知れないものとなります。さらに、（1）の事例のように、冒認出願までされた場合には、その内容が公開されてしまい、もはや「秘密」ではなくなってしまう上に、この事例のように、権利を取り戻すことができなければ、第三者の使用をやめさせることもできません。

このような営業秘密の被害の性質を踏まえると、漏えい後の法的手段によっては被害を十分に回復することができず、事前の漏えい防止、すなわち、いかに

[5] http://www.iprchn.com/Index_NewsContent.aspx?NewsId=137060

自社の営業秘密を漏えいから保護するかが極めて重要であることが理解できます。

3．中国における営業秘密侵害の典型パターン

第 1 節では、どのようにして営業秘密が漏えいしているかに関して、中国で近年増えている SNS アプリを通じた漏えいパターンを説明しました。本節では、どこから営業秘密が漏えいしているかについて、従来からの典型パターンを説明します。

（1）従業員漏えい型

これは、企業が雇用した従業員が、在職中または退職後に、企業の営業秘密を漏えいするというパターンです。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ます。本節で挙げる 3 パターンの中では、従来から、中国ではこの従業員漏えい型が最も多くを占めているようです。

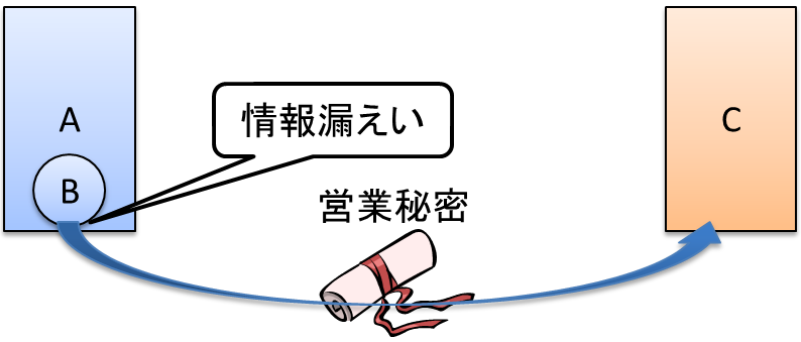
従業員漏えい型は、さらに、次の 4 つのパターンに分類することができます。

① 従業員が在職中に営業秘密を競合企業等に漏洩
② 従業員が退職後、転職先の企業に営業秘密を漏洩
③ 従業員が自ら競合会社を設立して、営業秘密を流用
④ 従業員の過失による漏えい

以下、順にみていきます。

① 従業員が在職中に営業秘密を競合企業等に漏洩

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す。



例えば、2021 年、最高人民法院が認定した損害額（1.59 億元）が、当時、中国最高額として注目された「バニリン事件」では、化学系企業（上図で A に相当）のバニリン製造現場の副主任として、関連設備のメンテナンス等を担当していた元従業員（上図で B に相当）が在職中、競合会社（上図で C に相当）から 40 万元の報酬を受け取り、バニリンの製造技術に関する営業秘密を提供しました。競合会社 C はその翌年からバニリンの製造を開始し、その後、グループ企業でバニリンの世界シェアの 1 割を占めるようになる一方で、A 社の世界シェアは 6 割から 5 割に低下した、という事案です。その他、この事件の詳細については、第 II 章 6. 参考裁判例でも説明します。

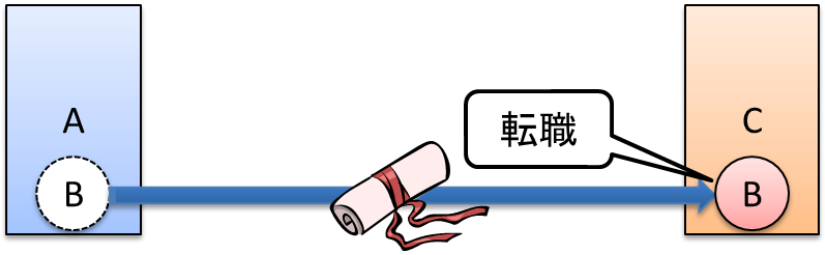
なお、このパターンの漏えい事件は、日本本社の従業員から中国の競合企業への漏えいという形でも発生しており、例えば、2020 年には、大手化学メーカの積水化学工業の元社員が、在職中に、スマートフォンのタッチパネル等に使用される技術情報を中国企業に漏えいした疑いで書類送検されています。日本本社から外国企業への漏えいについては、日本の「秘密情報の保護ハンドブック」（以下「ハンドブック」という。）[6]P.34～40 も参照してください。

---

[6] 経済産業省が公表している「秘密情報の保護ハンドブック（令和 6 年 2 月改訂版）」では、企業だけでなく、大学・研究機関等が保有している営業秘密を含む様々な秘密情報（個人情報、機微技術情報など）の漏えい対策（事故の予防に向けた日頃の対策と事故時の対応策）について、網羅的な解説を行っています（https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf）。また、同ハンドブックのポイントを簡潔にまとめた入門編・ガイダンス編となる「秘密情報の保護ハンドブックのてびき」（https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/170607_hbtebiki.pdf）も公開されており、あわせて参照されると有益です。

② 従業員が退職後、転職先の企業に営業秘密を漏洩

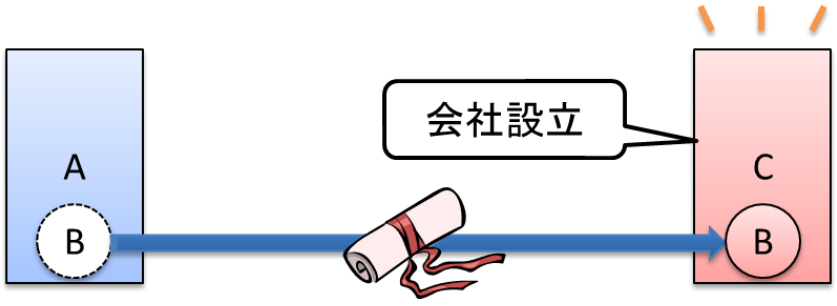
これは、自社（A社）の従業員Bが、A社を退職して競合企業C社に転職し、C社にて前勤務先のA社の営業秘密を利用したり、開示したりするパターンです。



例えば、中国の大手食品メーカ（上図でAに該当）では、10 年以上在職した従業員（上図でBに該当）が、退職後、秘密保持契約及び競業避止義務契約に違反して、偽名を使って競合メーカ（上図でCに該当）に就職し、ある食品の製造にかかる営業秘密を漏えいしたという事件が発生しています。なお、この営業秘密侵害行為によって、当該食品メーカには、1,000 万元余りの損害が発生したと言われています。

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す。



前節で取り上げた、２つの日系企業の被害例がまさにこの類型に該当します。この事例のように、元従業員が工場を設立して、侵害した営業秘密を利用するパ

ターンは、日本ではあまり見受けられないですが、**中国では良くあるパターン**です。

なお、第Ⅱ章5（1）(ii) で言及した判例（(2022)最高法知民終275号（最高人民法院2022年11月24日判決）では、従業員（上図B）がA社に就職する前に、A社とは事業分野が直接競合しないC社を設立していましたが、Bは在職中にA社の営業秘密を不正に入手し、退職。その後、C社はA社製品と同種製品を製造販売し始め、競合会社に転じた、というケースもあります。

④ 従業員の過失による漏えい

このパターンは、さらに

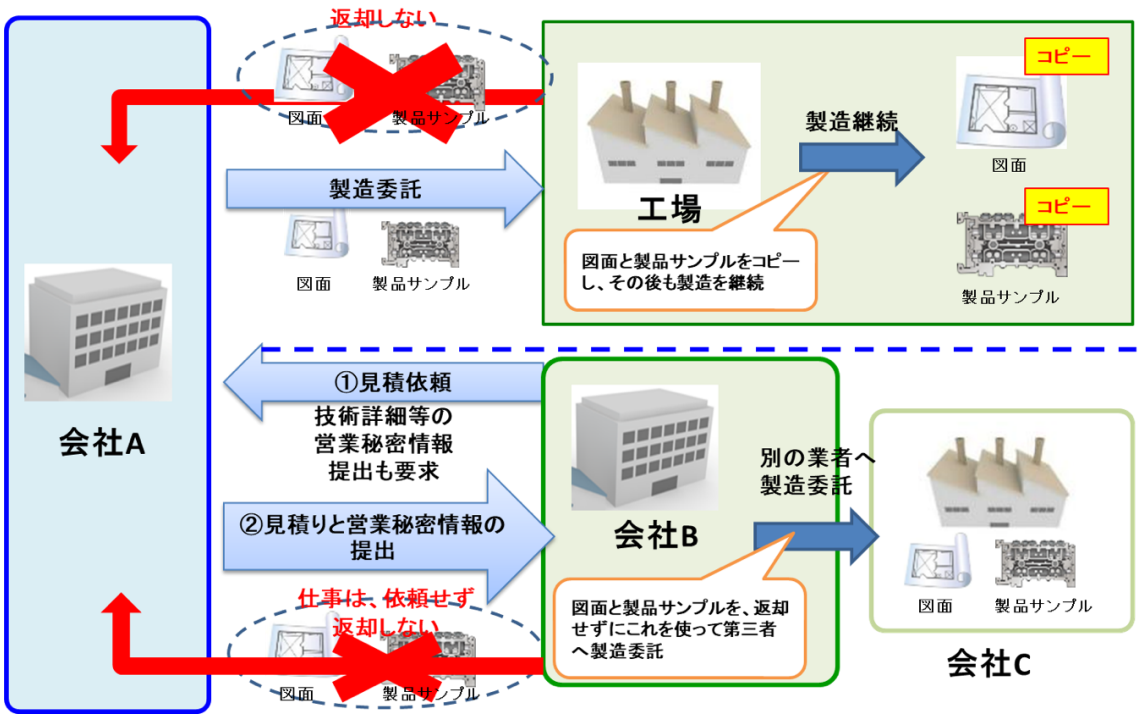
- 従業員が、何が営業秘密に該当するか分かっていない、又は、営業秘密の保護として自分たちが何をやれば良いのか、逆に、何をしてはいけないのかを理解できておらず、ショート動画アプリ等で営業秘密を含むような動画を投稿してしまうパターン
- 従業員が、業務の過程で、WeChatでの誤送信等により、誤って営業秘密を漏えいするパターン

に分けられます。

前者については、従業員への研修や部署内での営業秘密についての認識共有等が必要であり、後者については、誤送信が発生しやすいWeChatの業務使用を制限することが考えられます（第Ⅲ章参照）。

（2）取引先漏えい型

このパターンは、下請けまたは顧客、ライセンシーといった、取引先から営業秘密が漏えいするというパターンです。



①委託先から営業秘密が漏えいするパターン（上図上段参照）

このパターンには、例えば、中国企業に金型等の製造を委託する場合、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します。

②顧客から営業秘密が漏えいするパターン（上図下段参照）

このパターンには、例えば、顧客である中国企業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社がそれらを別の中国企業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します。

　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と、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基本的に必要ですが、これは、後述する立証責任の転換規定によっても、一般的には難しいと考えられます。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専利権（特許権や実用新案権）などの登録権利に基づき、C社に対して権利行使を行うことを検討すべきです。

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、専利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つの製品を多角的にあらゆる知的財産によって保護するという視点が、非常に重要となってきます。

③　業務提携先・ライセンシーから漏えいするパターン

このパターンは、業務提携先・ライセンシーが提携期間中、契約に違反して営業秘密を漏えいする、または、提携関係・ライセンス契約終了後も無断で営業秘密を使用し続けるといったケースが該当します。

例えば、あるミニプログラムのソースコードを開発した会社が、業務提携先に対し、その使用許諾契約を締結した上で、当該ソースコードを提供したところ、提携先は契約上の秘密保持義務に違反し、当該ソースコードをオープンソースソフトウェアとしてネットワーク上に公開したという事例が挙げられます。当該ソースコードの公開後、開発会社のミニプログラムの売上高は、ピーク時の約1/3まで減少したとのことです。その他、この類型については、第Ⅱ章の参考裁判例（３）も参照してください。

なお、このパターンには、（１）の従業員漏えい型に近いですが、提携先の従業員が競合先に漏えいするというケースも含まれ、日本でもこのパターンの漏えい事件が発生しています。例えば、2014年、東芝のパートナー企業であるサンディスクの元技術者が、東芝の半導体メモリに係る研究データを不正に持ち出し、韓国の半導体メーカに提供した疑いで逮捕されています。

業務提携の前には、相手方のコンプライアンス意識や、従業員管理を含めた営業秘密管理体制についても、信用できるか否かを可能な限り確認することが望ましいです（第Ⅲ章参照）。

（３）第三者不正取得型

このパターンは、従業員等以外の第三者により、窃盗、賄賂、詐欺、脅迫等、不正手段により、権利者の営業秘密を獲得するというものであり、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します。ただし、（1）の従業員漏洩型に比べて実際の事例に占める割合は低く、また、対策としては、一般的な防犯・セキュリティ管理及び従業員漏洩型の防止と重複するものと考えられます。

第２章　法制度編

本章のポイント

- 法律上、営業秘密とは、①非公知性、②価値性、③管理性を有する商業情報のことである。
- 上記①～③のうち、特に、③管理性（営業秘密に管理措置を講じること）が実務上、重要となる。具体的な措置の例は、司法解釈の規定が参考になるが、実際に営業秘密の漏えいを防ぐためには、さらに対策を考える必要がある（⇒第Ⅲ章）。
- 営業秘密侵害行為に対しては、民事・行政・刑事の３つの法的手段を採ることができる。実務上は技術関連の営業秘密侵害については、民事又は刑事が利用される傾向にあるが、後者は訴追基準が規定されている。
- 民事手続きにおいては、証拠収集の困難性を考慮した制度が、法律及び関連する司法解釈に規定されている。

１．中国における営業秘密の定義

本章では、まず、「営業秘密」とは何か、法律上の定義に即して説明します。

「営業秘密」の保護については、国際的には、WTO・TRIPs 協定（知的所有権の貿易関連側面協定）において規定されており、日本や中国などを含めて、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ります。 このため、中国における営業秘密の法律上の定義は、日本法における定義と良く似ています。

下表は、中国における営業秘密の法律上の定義を、日本法と比較して整理したものです。

	中　国	日　本
根拠法	反不正当競争法	不正競争防止法

定義規定	公衆に知られていない、商業的価値を有し、かつ、権利者が関連の秘密保護措置をとった技術情報、経営情報等の商業情報（第 9 条第 4 項)。	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（第 2 条第 6 項)
要件①：非公知性	公衆に知られていないこと	公然と知られていないこと
要件②：価値性／有用性	商業的価値を有すること	事業活動に有用であること
要件③：秘密管理性	権利者が相応の秘密保護措置をとったこと	秘密として管理されていること
情報の種類	技術情報、経営情報等の商業情報	技術上又は営業上の情報

TRIPs 協定の第 39 条第 2 項には、営業秘密の保護に関連して、開示されていない情報についての要件として、「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」の 3 つの要件が規定されており、日本法も中国法も、この 3 つの要件－①非公知性、②価値性／有用性、③秘密管理性を規定しています。

なお、中国の反不正当競争法は、1993 年に制定された後、2017 年及び 2019 年に改正されていますが、2017 年の改正前は、要件②価値性／有用性に関しては、「権利者に経済的な価値をもたらし、実用性を有する」と規定されており、また、情報の種類についても、「技術情報及び経営情報」に限定されていました。これが、まず、2017 年の法改正により、要件②価値性／有用性が「商業的価値を有し」に変更され、さらに 2019 年の法改正により、保護対象となる情報の種類が「技術情報、経営情報等の商業情報」と拡大されました。

このように、中国法における営業秘密の定義は、日本法における定義と概ね同じであり、日本において営業秘密として扱う情報は、中国においても営業秘密として管理することを考える必要があります。

2．法律上の 3 要件－非公知性・価値性・管理性について

中国では、各法律の規定について、「**司法解釈**」という、最高人民法院等による具体的判断基準その他の法律問題についての具体的な解釈規定が多数公布されており、営業秘密の反不正当競争法上の 3 要件―①非公知性、②価値性、③管理性についても、司法解釈**「最高人民法院による営業秘密侵害民事事件の審理における法律適用の若干問題に関する規定」**（法釈〔2020〕7 号。以下、本章ではこの法釈番号のみ示します。）により具体的な規定があるため、ここでは、この司法解釈に沿って、3 要件についてより詳しく説明します。なお、この司法解釈は、そのタイトル通り、民事事件への適用を前提としたものですが、これらの 3 要件についての考え方は、基本的には、行政事件、刑事事件においても同様であると考えられます。

2019 年の反不正当競争法の改正により、営業秘密侵害に係る民事訴訟においては、権利者が「秘密管理性」要件を初歩的な証拠により証明し、かつ、相手方の侵害行為を合理的に表明した場合には、被疑侵害者が営業秘密に該当しないことを証明しなければならない旨の規定が新設されました(32 条)。したがって、**権利者の立場からは、3 要件の中でも、特に③管理性要件を満たすこと、また、そのことを証拠として提出し得る形で整備しておくことが、さらに重要となった**ということができます。

（1）非公知性

非公知性―「公衆に知られていない」とは、「被疑侵害行為の発生時点で当業者に普遍的に知られておらず、簡単に獲得できないもの」をいいます。したがって、次のような場合には、一般的には、非公知性の要件を満たさないこととなります（法釈〔2020〕7 号第 3 条、第 4 条第 1 項参照)。

（一）当該情報が、当分野において一般常識又は業界慣行に属するものである場合

（二）当該情報が、製品の寸法、構造、材料、部品の簡単な組合せ等の内容のみに係るものであり、当業者が市販されている製品を観察することで直接獲得できる場合
（三）当該情報が、公開された出版物又はその他のメディアで公然開示されたものである場合
（四）当該情報が、公開された報告会、展覧等の方法により公開されたものである場合
（五）当業者が他の公開ルートで当該情報を獲得できる場合

ただし、ベースとする情報自体は既に公衆に知られている場合でも、その情報を整理、改善、加工して形成された新たな情報については、「被疑侵害行為の発生時点で当業者に普遍的に知られておらず、簡単に獲得できないもの」である場合には、非公知であるとされます（同第 4 条第 2 項)。

（2）価値性

価値性―「商業的価値を有する」とは、権利者が保護を求める情報が公衆に知られていないがゆえに、現実的又は潜在的な商業的価値を有することをいいます（法釈〔2020〕7 号第 7 条第 1 項)。このように、潜在的な価値を有していれば、実際に価値を発揮しているか否かは問わず、また、2017 年の反不正当競争法の改正により、「実用性を有する」が要件から削除されたことから、その情報が事業活動に実際に利用されるか否かも問わないと考えられます。生産経営活動において形成される段階的な成果もまた、これに該当し得るものです（同 7 条第 2 項)。

（3）管理性

管理性―「権利者が相応の秘密保護措置をとったこと」とは、権利者が営業秘密の漏洩を防止するために、被疑侵害行為の発生前に合理的な秘密保持措置を講じたことを意味し、これは、営業秘密及びその媒体の性質、営業秘密の商業的価値、秘密保持措置の識別度、秘密保持措置と営業秘密との対応の程度及び権利者の秘密保持の意思等の要素に基づき判断されます（法釈〔2020〕7 号第 5 条第 1 項、2 項)。

具体的にどのような措置を講じれば良いのかについても、同司法解釈の規定が参考になります。第６条には次のように規定されています。

次の各号に掲げる状況のいずれかに該当し、通常、営業秘密の漏洩を防止するのに十分である場合、人民法院は、権利者が相応の秘密保持措置を講じたと認定しなければならない。

（一）秘密保持合意書を締結したか又は契約において秘密保持義務を取り決めた場合
（二）定款、教育、規則制度、書面告知等の方式により、営業秘密に接し、営業秘密を獲得できる従業員、元従業員、サプライヤー、顧客、訪問者等に対して秘密保持を要請した場合
（三）秘密に係る工場、作業場等の生産経営場所について訪問者を制限したか又は区分管理を行った場合
（四）表示、区分、隔離、暗号化、密封保存、接触又は獲得できる人員範囲の制限等の方式で、営業秘密及びその媒体を区分・管理した場合
（五）営業秘密に接し、営業秘密を獲得できるコンピューター設備、電子装置、ネットワーク設備、保存設備、ソフトウェア等について使用、アクセス、保存、複製の禁止又は制限等の措置を講じた場合
（六）退職する社員に対し、接触又は獲得した営業秘密及びその媒体を登記、返却、消去、廃棄し、引き続き秘密保持義務を履行するよう要請した場合
（七）その他の合理的な秘密保持措置を講じた場合

いずれも、営業秘密の管理の基本ともいうべき措置であり、日本法の考え方とそれほど変わらないことが分かります。ただし、これはあくまで、当該情報が法律上、営業秘密として認められるための要件であって、実際に営業秘密の漏えいを防ぐためには、第Ⅲ章で説明するように、さらに対策を考える必要があります。

３．中国における営業秘密侵害行為の定義

反不正当競争法上、営業秘密侵害行為は次のように定義されています（第９条第１項各号）。

- 窃盗、賄賂、詐欺、脅迫、電子的手段による侵入又はその他の不正手段をもって権利者の営業秘密を獲得すること。
- 前号に定める手段を用いて獲得した権利者の営業秘密を開示、使用し又は他人に使用を許諾すること。
- 秘密保持義務又は権利者の営業秘密保持に関する要求事項に違反して保有している営業秘密を開示、使用し、或いは他人に使用を許諾すること。
- 秘密保持義務又は権利者の営業秘密保持に関する要求事項に違反するよう他人を教唆、誘惑、幇助して権利者の営業秘密を獲得、開示、使用し又は他人に使用を許諾すること。

下表は、中国における法律上の営業秘密侵害行為の類型を、日本法と比較して整理したものです。

<table>
<tr><th></th><th>中　国</th><th>日　本</th></tr>
<tr><td>根拠法</td><td>反不正当競争法（第９条）</td><td>不正競争防止法（第２条／以下では、中国法に対応する条文のみ抜粋）</td></tr>
<tr><td rowspan="2">不正手段による取得／開示</td><td>窃盗、賄賂、詐欺、脅迫、電子的手段による侵入又はその他の不正手段（※１）をもって権利者の営業秘密を獲得すること</td><td rowspan="2">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（秘密を保持しつつ特定の者に示すことを含む。）</td></tr>
<tr><td>前号に定める手段を用いて獲得した権利者の営業秘密を開示、使用（※２）し又は他人に使用を許諾すること</td></tr>
<tr><td>不正開示</td><td>秘密保持義務（※３）又は権利者の営業秘密保持に関する要求事項に違反して保有して</td><td>営業秘密を保有する事業者（以下「営業秘密保有者」という。）からその営業秘密を</td></tr>
</table>

	いる営業秘密を開示、使用し、或いは他人に使用を許諾すること	示された場合において、不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、その営業秘密を使用し、又は開示する行為
		その営業秘密について営業秘密不正開示行為（前号に規定する場合において同号に規定する目的でその営業秘密を開示する行為又は秘密を守る法律上の義務に違反してその営業秘密を開示する行為をいう。以下同じ。）であること若しくはその営業秘密について営業秘密不正開示行為が介在したことを知って、若しくは重大な過失により知らないで営業秘密を取得し、又はその取得した営業秘密を使用し、若しくは開示する行為
教唆・幇助	秘密保持義務又は権利者の営業秘密保持に関する要求事項に違反するよう他人を教唆、誘惑、幇助して権利者の営業秘密を獲得、開示、使用し又は他人に使用を許諾すること	（民法第 719 条、刑法第 61 条、第 62 条）

※１：不正手段による取得について規定する第 1 号における「その他の不正手段」とは、「法律の定め若しくは一般に認められる商業道徳に違反する方法」をいう（法釈〔2020〕7 号第 8 条）。

※２：営業秘密の「使用」には、被疑侵害者が生産経営活動において営業秘密を直接使用した場合のほか、営業秘密を修正・改良した後に使用した場合、

又は営業秘密に基づき関連生産経営活動を見直し、最適化し、改良した場合も含まれる（法釈〔2020〕7 号第 9 条）

※３：「秘密保持義務」は、当事者が法律の定め又は契約の取り決めに基づいて負う秘密保持義務のことである。ただし、当事者が契約において秘密保持義務を取り決めなかった場合であっても、信義誠実の原則及び契約の性質、目的、契約成立のプロセス、取引習慣等に基づけば、被疑侵害者が、獲得した情報が権利者の営業秘密であることを知っている場合又は知るべきである場合は、秘密保持義務を負うものと認められる（法釈〔2020〕7 号第 10 条）。

なお、第三者は、営業秘密の権利者の従業員、元従業員又はその他組織、個人が第 1 項に掲げた違法行為を実施したことを知りながら又は知るべきであるにもかかわらず、当該営業秘密を獲得、開示、使用し、又は他人に使用を許諾した場合、営業秘密を侵害する行為とみなされます（反不正当競争法第 9 条第 3 項）。日本の不正競争防止法第 2 条第 1 項第 5 号、8 号に相当する規定ですが、同第 6 号、9 号（事後的な知得等に関する規定）に相当する明文規定はありません。

Step Up!

リバースエンジニアリング

日本法の下では、いわゆる「リバースエンジニアリング」は、営業秘密の３要件のうちの①非公知性に関連して議論されることが多いと思います。
これに対して中国では、リバースエンジニアリングは、営業秘密侵害行為に該当しないことが、以下のように、司法解釈に規定されています。

「最高人民法院による営業秘密侵害民事事件の審理における法律適用の若干問題に関する規定」第 14 条

自主研究開発又はリバースエンジニアリングを通じて被疑侵害情報を獲得した場合、人民法院は、反不正競争法第九条に定める「営業秘密侵害行為」に該当しないと認定しなければならない。
前項にいう「リバースエンジニアリング」とは、技術的手段を通じて公開ルートから取得された製品に対して分解、測定・製図、分析等を行うことで当該製品の関連技術情報を取得することをいう。
被疑侵害者が不正手段により権利者の営業秘密を獲得した後に、リバースエンジニアリングを理由として営業秘密を侵害していないと主張した場合、人民法院は、これを支持しない。

上記規定からも分かるように、実務では被告側の抗弁事由となります。

では、「リバースエンジニアリング」を禁止する規定などによって、かかる抗弁を封じることはできるのでしょうか？
まず、このようなリバースエンジニアリング禁止条項自体の有効性は否定されないと考えられます。例えば、ソフトウェアの著作権許諾契約におけるリバースエンジニアリング禁止条項について、「中国の法律は当事者がライセンス契約におけるリバースエンジニアリング禁止条項を禁止していない。」と判示して、契約違反であるとする著作権者の主張を認めた裁判例[7]も存在します。

しかし、製品が市場で不特定の需要者間で流通する場合には、このような禁止規定等のみでは、そもそも、営業秘密該当性（2019 年の反不正当競争法改正後は特に管理性要件の充足性）が否定される可能性があります。
「秘密保持の目的で採用する秘密保護措置は、不特定の第三者がリバースエンジニアリングを通じてその技術秘密を取得することに対抗し得るものである必要がある。（製品に付された）ラベルは安全上の注意書き、修理保証の注意書きに属するものであり、・・・たとえ『営業秘密を含む。破壊厳禁』等の秘密保護目的の記載であっても、他人のリバースエンジニアリングに対抗できる物理的な秘密保護措置を構成しない。市場での流通により製品を取得した不特定の第三者は権利者と契約関係になく、製品を分解しないという契約上の義務を負う必要はない一方で、当該製品を所有権に基づいて処分する権利を有しており、権利者の一方的な宣言に拘束されない。」として、管理性要件の充足を否定した判例もあります[8]。

以上の裁判例からすると、不特定の第三者の間で流通する製品については、例えば、技術内容を保護する暗号化や、製品を分解等すると営業秘密も取得できなくなるような構造とすることにより、物理的に営業秘密を保護するしくみを採用すること、逆に、そうした措置を講じることができない場合には、特許や実用新案などの登録権利によって技術内容を保護することを考えることが望ましいでしょう。
一方、特定の相手方に営業秘密を含む製品を提供する場合、その取引契約（売買契約等）において、秘密保持義務規定及びリバースエンジニアリング禁止規定を設けること、また、上述の物理的措置のほか、かかるリバースエンジニアリング条項に違反したことが容易に分かるような物理的な手段があれば、それもあわせて講じることが望ましいと考えられます。

４．侵害行為に対する救済

[7] (2012)高民終字第 868 号（北京市高級人民法院 2013 年 6 月 20 日判決）
[8] (2020)最高法知民終 538 号（最高人民法院 2020 年 12 月 14 日判決）

中国においては、営業秘密侵害行為に対しては、民事救済、行政処分、刑事制裁の３つの手段をとることができます。営業秘密侵害行為が行政処罰の対象となる点が日本と異なります。

	中国	日本
民事救済	・当事者間（権利者・侵害者）の民事訴訟 ・侵害行為の差止、侵害行為の組成物（営業秘密記録媒体等）の廃棄及び損害賠償請求が可能[9] ・訴訟時効は、権利者がその権利が侵害されたこと及び義務者を知った日又は知りうべき日から３年（除斥期間は損害を受けた日から 20 年）。（民法典第 188 条）。	・当事者間（権利者・侵害者）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 ・営業秘密侵害に係る差止請求権・損害賠償請求権の消滅時効は、侵害の事実及びその行為を行う者を知った時から３年、又は行為の開始の時から 20 年。
行政処分	・行政機関（市場監督管理局）による摘発 ・行政処分の内容は、侵害行為の停止、違法所得の没収、過料	なし
刑事制裁	・刑事摘発後、起訴されれば刑事訴訟に移行 ・公訴時効は 15 年（刑法第 219 条、87 条）。 ・刑事罰の内容は、３年以下の懲役及び／または罰金。	・捜査後、起訴されれば刑事訴訟に移行。 ・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。 ・公訴時効は７年

[9] その他、謝罪請求等が可能です（民法典第 179 条）。

	特に情状が重大な場合は、3年以上 10 年以下の懲役に罰金刑を併科。	

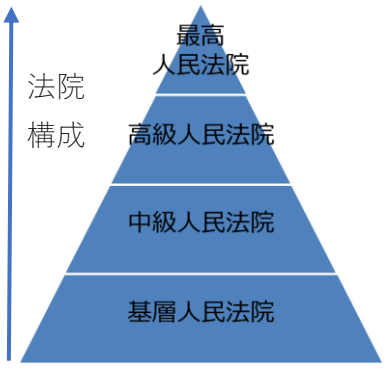
以下、それぞれについて概説します。

（1）民事救済

民事救済とは、営業秘密侵害者に対して、民事訴訟を提起して、侵害行為の差止めと損害賠償を求める救済手段です。

中国の訴訟は二審制であり、営業秘密侵害に係る民事訴訟のうち、技術関連の事件については、第一審は中級人民法院の管轄となり、それ以外の事件の第一審は基層人民法院の管轄となります（「最高人民法院による第一審知的財産権に係る民事および行政案件の管轄に関する若干規定」法釈［2022］13 号第 1 条、3 条）。また、第二審は技術関連の事件のうち、重大で複雑な事件は最高人民法院の知的財産法廷が審理し（「最高人民法院による知的財産権法廷の若干問題に関する規定」法釈［2023］10 号第 2 条第 1 項第 3 号）、それ以外の技術関連の事件は高級人民法院が審理を行い、技術関連以外の事件は、中級人民法院の管轄となります（下表参照）。

	技術関連の営業秘密侵害事件		非・技術関連の営業秘密（経営情報等）侵害事件
第一審	中級人民法院		基層人民法院
第二審	重大で複雑な事件	最高人民法院（知的財産法廷）	中級人民法院
	上記以外の事件	高級人民法院	



営業秘密侵害民事事件の管轄

民事訴訟において、損害賠償を請求する場合、その額は、以下の①～③を基準に、その順序に従って算定されることになります（反不正当競争法第 17 条）。

① 権利侵害行為によって被った実際の損害に基づき算定
② 侵害者が権利侵害行為によって得た利益に基づき算定
③ 権利侵害行為の情状に基づき、500 万元以下の賠償額を算定

このうちの③の算定方式により損害賠償額を認定する方式は、「法定賠償」と呼ばれ、実際の訴訟では、①、②の証拠に基づく立証が一般的に困難であるために、この法定賠償方式により算定されるケースが多いです。

なお、上記①、②の算定方法による場合において、侵害行為が悪意で実施され、情状が重大である場合は、これらの基準で算定される金額の１倍以上５倍以下で賠償額を確定することができる、いわゆる「懲罰的賠償制度」が適用される可能性もあります。

（２）行政処分

「行政摘発」とも称される行政処分とは、行政機関による差止め、過料等の行政処分であり、営業秘密侵害については、各地の市場監督管理局が管轄の行政機関となります。

行政処分の内容は、侵害行為の停止命令、違法所得の没収、過料であり、過料の額は、原則として１０万元以上１００万元以下であり、情状が重大な場合には、５０万元以上５００万元以下とされています（反不正当競争法第 21 条）。

なお、行政摘発後に、侵害者に対して民事訴訟を提起して、損害賠償請求することも可能です。また、被害規模等に応じて、行政機関の判断で、後述の刑事制裁の対象として刑事手続きに移送されることもあります。

実務上は、経営情報に係る営業秘密侵害事件について利用される傾向にあるといえます（第Ⅲ章参照）。

（３）刑事制裁

刑事制裁は、公安当局による捜査（刑事摘発）の後、起訴された場合には刑事訴訟に移行し、刑事訴訟において有罪判決（第一審の管轄は基層人民法院、第二審の管轄は中級人民法院となる。）が確定すれば、刑事罰による制裁を侵害者に課すことで保護の実効性を図る法的措置です。

2020 年の刑法改正により、営業秘密侵害罪は厳罰化されており、具体的には、次のような規定となりました（刑法第 219 条）。

以下の営業秘密侵害行為の一に該当し、 ① 窃盗、賄賂、詐欺、脅迫、電子的侵入又はその他の不正手段をもって権利

者の営業秘密を取得した場合
② 前号の手段で取得した権利者の営業秘密を開示し、使用し又は他人に使用を許諾した場合
③ 秘密保持義務に違反し又は権利者の営業秘密保持に関する要求に違反し、その掌握する営業秘密を開示し、使用し又は他人に使用を許諾した場合

かつ、情状が重大な場合には、3 年以下の有期懲役に処し、罰金を併科又は単科すると規定され、情状が特に重大な場合には、3 年以上 10 年以下の有期懲役に処し、かつ罰金を併科する。

※なお、前記各号の行為を知りながら、当該営業秘密を取得、開示、使用又は他人に使用を許諾した場合には、営業秘密侵害とされる（2 項)。

「情状が重大な場合」及び「情状が特に重大な場合」の基準については、司法解釈の改正も進められており、その草案では、「情状が重大な場合」として、「権利者に 30 万元以上の損失をもたらした場合」等が、「情状が特に重大な場合」として、「権利者にもたらした損失額または営業秘密侵害による違法所得額が 250 万元以上」と規定されています（「知的財産権侵害刑事事件の処理における法律適用に関する若干問題の解釈」（意見募集稿）第 14 条)。

また、刑法の改正にあわせて、刑事訴追基準に関する司法解釈（「最高人民検察院、公安部による公安機関の管轄する刑事事件の立件・訴追基準に関する規定（二)」）も以下のように改正されています（「最高人民検察院、公安部による営業秘密侵害刑事事件の立件・訴追基準の修正に関する決定」)。

① 営業秘密権利者にもたらした損失額が ３０万元以上の場合
② 営業秘密侵害者による違法所得額が ３０万元以上の場合
③ 営業秘密権利者に直接的に重大な経営難をもたらし、それにより破産、倒産が生じた場合
④ その他、営業秘密権利者に重大な損失をもたらした場合

従来は、刑法上の犯罪の構成要件である、重大な損失／特に重大な結果（現行法における「情状が重大」、「情状が特に重大」に相当）の判断基準と、刑事訴追基準が一致していませんでしたが、刑法改正と前後して行われた司法解釈の改正[10]により、損失額／違法所得額の基準が統一されることとなりました。

刑事罰の内容は、3 年以下の有期懲役及び／または罰金です。情状が特に重大な場合には、3 年以上１０年以下の有期懲役に処され、かつ罰金が併科されます（刑法第 219 条）。

罰金額は、通常、違法所得額の 1 倍以上 5 倍以下で確定されます。違法所得額が明らかにできない場合には、不法経営額の 50%以上 1 倍以下で確定されます。違法所得額も不法経営額も明らかにできない場合であって、3 年以上の有期懲役を科す場合には、15 万元以上 500 万元以下の罰金額となり、それ以外の場合には、3 万元以上 100 万元以下の罰金額となります（「最高人民法院、最高人民検察院による知的財産権侵害刑事事件の処理における具体的な法律適用に関する若干問題の解釈（三）」法釈〔2020〕10 号第 10 条第 2 項）。

なお、刑事制裁を利用しつつ、「附帯民事請求」[11]による損害賠償請求も可能であり、刑事摘発を利用して必要な証拠を収集した上で、刑事訴訟判決後に、別途、民事訴訟を提起して、損害賠償を請求することも可能です。

５．民事手続きにおける諸制度

前節では、中国における営業秘密侵害に対して採りうる 3 つの法的手段―民事救済、行政処分、刑事制裁の概要について説明しました。これらの 3 つの法的手段のうち、行政処分と刑事制裁については、それぞれ、行政機関、公安当局に

---

[10] 本文で紹介した司法解釈の草案のほか、2020 年刑法改正前の「重大な損失」、「特に重大な結果」の用語がそのまま用いられていますが、執筆時時点で有効な司法解釈（「最高人民法院、最高人民検察院による知的財産権侵害刑事事件の処理における具体的な法律適用に関する若干問題の解釈（三）」法釈〔2020〕10 号）においても、同じ損失額／違法所得額が規定されています。

[11] 附帯民事訴訟とは、犯罪行為により物質的損害を受けた被害者が、刑事訴訟の過程で、その賠償等を求めて提起することができる民事訴訟のことです（刑事訴訟法第 101 条）。

て捜査と証拠収集が行われますが、民事救済においては、民事訴訟を提起する権利者の側で証拠収集を行い、侵害事実を立証しなければなりません。しかし、営業秘密侵害事案においては、相手方の工場等の内部で侵害行為が行われているケースも多く、他の知的財産権侵害の場合と比べて、侵害行為の証拠の収集や侵害行為の立証が困難であることが多いです。このため、民事訴訟に関しては、反不正当競争法や関連する司法解釈において、証拠収集や立証責任の負担を軽減するための制度がいくつか存在します。本節では、かかる制度について説明します。

（1）立証責任の負担軽減に関する法規定

(i) 営業秘密該当性の立証についての規定

営業秘密の法律上の 3 要件については、第 2 節で説明した通りです。営業秘密侵害の民事訴訟においては、権利者が、侵害されたと主張する情報が法律上の営業秘密に該当することを主張立証しなければなりません。この点について、2019 年の反不正当競争法の改正により、以下の規定が追加されました（第 32 条第 1 項）。

> 営業秘密侵害に係る民事訴訟手続きにおいて、営業秘密の権利者が初歩的な証拠を提出し、主張する営業秘密に対して秘密保護措置を講じたことを証明し、かつ営業秘密が侵害されたことの合理的な表明を行った場合は、被疑侵害者は権利者が主張した営業秘密が本法に規定される営業秘密に属さないことを証明しなければならない。

本規定によれば、権利者は、営業秘密の該当性については、3 要件のうち、③管理性について立証すれば、他の 2 要件（①非公知性、②価値性）のいずれかを備えないことを、被疑侵害者側が立証しなければならないことになります。すなわち、繰り返しになりますが、権利者にとっては、秘密情報の管理措置を講じること、そしてその措置が秘密管理性要件をクリアし得るレベルであることが重要であることは言うまでもないのですが、そのことを証拠として提出し得る形で整備しておくことが、より重要となったということです。

(ii) 侵害行為の立証についての規定

2019 年の改正反不正当競争法では、侵害行為の立証責任の転換についての規定も追加されました（第 32 条第 2 項）。

営業秘密の権利者が初歩的な証拠を提出して営業秘密が侵害されたことを合理的に表明し、かつ、以下の証拠のいずれかを提出する場合、被疑侵害者は営業秘密侵害行為が存在しないことを証明しなければならない。

（1）被疑侵害者が営業秘密を獲得するルート又は機会があり、被疑侵害者が使用する情報が当該営業秘密と実質的に同一であることを表明する証拠。

（2）営業秘密が被疑侵害者によりすでに開示、使用され、又は開示、使用されるおそれがあることを表明する証拠。

(3) 営業秘密が被疑侵害者に侵害されたことを表明するその他の証拠。

本規定の（1）から（3）は、いずれも、相手方による営業秘密侵害行為の存在を間接的に裏付ける証拠であり、通常、柱書前半の「初歩的な証拠」を兼ねるものと考えられます。すなわち、一般的には、上記（１）から（３）に規定する証拠を提出できた場合には、営業秘密侵害行為についての立証責任が転換されると考えられます。

なお、（１）の**「営業秘密を獲得するルート又は機会」に関して、被疑侵害者が従業員、元従業員である場合**には、以下の要素が考慮され得ることになります（「最高人民法院による営業秘密侵害民事事件の審理における法律適用の若干問題に関する規定」法釈〔2020〕7 号第 12 条）。

（一）役職、職責、権限

（二）本業である仕事又は職場から割り振られた任務

（三）営業秘密に係る生産経営活動に関与した具体的な状況

（四）営業秘密及びその媒体を保管、使用、保存、複製、支配したか又はその他の方式で接触、獲得したか否か

（五）その他

また、同じく（１）の「当該営業秘密と実質的に同一」とは、当該営業秘密と実質的に区別がない場合を意味し、具体的には、以下の要素に基づき判断されます（法釈〔2020〕7 号第 13 条）。

（一）被疑侵害情報と営業秘密の異同の程度

（二）当業者が被疑侵害行為の発生時点で被疑侵害情報と営業秘密との区別を容易に想到するか否か

（三）被疑侵害情報と営業秘密の用途、使用方式、目的、効果等に実質的な差異があるか否か

（四）公的分野における営業秘密に関連する情報の状況

（五）その他

以上より、中国で多い類型と思われる、退職者による競合会社への営業秘密漏洩により類似製品が販売された事案を想定すると、例えば、在職中の被疑侵害者の職務内容を示す書類と、公証購入した競合会社の類似製品の分析結果等を証拠として（上記（１）：法 32 条 2 項 1 号）、あるいは、在職中の被疑侵害者のメールなどの交信記録を証拠として（上記（２）：法 32 条 2 項 2 号）、立証責任の転換を図ることになると考えられます。

実際の紛争では、上記（１）～（３）に関する証拠を幅広く収集することになると考えられます。

例えば、ある工業用特殊塗料の成分・配合等の営業秘密について、退職した元従業員（Y1）及びその設立会社（Y2）に対する営業秘密侵害訴訟[12]において、裁判所は以下のように判示して、**法第 32 条第 2 項第 2 号（上記（2））**の適用により、被告側に被告側に立証責任を転換し、結果として侵害行為を認めました。

「（本件塗料には）様々な成分及び配合比が存在し、・・・各顧客にあわせた処方を作成する必要があり、一定の研究開発投資と技術の蓄積がなければ、短期間で特定の顧客のニーズにあわせた塗料の開発は困難である。

（Y1 が原告会社に就職する前に設立した Y2 は、もともとの経営範囲が当該塗料とは無関係であったが、）Y1 が原告会社を退職してわずか 4 か月後に、Y2 は当該塗料の製造販売に転じている。・・・もし、原告会社の営業秘密に係る配合情報等がなければ、Y2 が短期間で同種製品を開発することは困難である。し

[12] (2022)最高法知民終 275 号（最高人民法院 2022 年 11 月 24 日判決）

たがって、Y1 が原告の許可なく営業秘密を取得して Y2 に開示し、Y2 が当該営業秘密を使用して同種製品を製造した、高度の蓋然性がある。」

判決を読む限り、上記の認定は、主に、

・原告会社の退職 4 か月後における、被告会社 Y2 の同種塗料の製品写真や機能紹介を含む WeChat のモーメンツ（第Ⅰ章１（1）参照）投稿

の証拠に基づいているようなのですが、原告はこのほかにも、原告は、以下のような、上記法第 32 条第 2 項第 1 号（1）の適用を意図したものと思われる証拠も提出していました。

・元従業員が、営業秘密が保存された原告会社の技術部門専用パソコンを使用したこと等の証拠として、原告会社の社員の通信記録及び証言
・被告会社が顧客に販売した塗料の成分とその配合率が、原告製品と高度に一致していることを示す分析報告書

（iii）損害額の算定における帳簿等の提出命令

日本法における文書提出命令の特則（不正競争防止法 7 条）に相当する規定も存在します。対象は、損害額の算定に関する帳簿や資料等であり、侵害行為の立証のための資料等は含まれていませんが、司法解釈に以下のような規定があります（法釈〔2020〕7 号第 24 条）。

権利者は、侵害者が侵害により獲得した利益について初歩的な証拠を提出しているが、営業秘密侵害行為に関する帳簿、資料が侵害者に掌握されている場合、人民法院は、権利者の申立により、侵害者に対して、当該帳簿、資料を提供するよう命じることができる。侵害者が正当な理由なく、提供を拒否し、又は、実際のとおりに提供しなかった場合、人民法院は、権利者の主張及び提出された証拠に基づき、侵害者が侵害により獲得した利益を認定することができる。

ただし、そもそも、「侵害者が侵害により獲得した利益についての初歩的な証拠」を提出することは容易でなく、前節で説明したように、実際には法定賠償に基づき損害額が算定されることになることがほとんどであると思われ、本規定が利用されるケースは限られると予想されます。

（2）証拠収集の負担軽減に関する制度―証拠保全

証拠保全とは、証拠が滅失または後日取得し難くなるおそれがある場合に、当事者の申立てにより、裁判所が必要な証拠の保全措置を取ることができる制度です（民事訴訟法 84 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、証拠保全は、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ます。

営業秘密侵害事件を含む、知的財産権侵害関連の民事訴訟における証拠保全については、司法解釈（**「最高人民法院による知的財産権に係る民事訴訟の証拠に関する若干の規定」法釈〔2019〕12 号**）に詳細な規定があります。

(i) 要件（第 11 条）

人民法院は、当事者または利害関係者による証拠保全の申立に対して、以下の要素を考慮して審査しなければならない。 （一）申立人がその主張に関する初歩的証拠を提出したかどうか （二）申立人が自ら証拠を収集することができるかどうか （三）証拠滅失または以後取得困難の可能性及びその要証事実の証明への影響 （四）講じうる保全措置による証拠保有者への影響

まず、第 1 号に規定されるように、証拠保全の申立ての際には、営業秘密侵害行為に関する初歩的な証拠の提出が必要です。なお、証拠保全申立てのための初歩的な証拠と、侵害行為の立証責任転換規定（反不正当競争法第 32 条第 2 項）の適用において必要とされる証拠は共通するものと考えられます。これとあわせて、申立ての際には、保全の必要性（2 号、3 号）や、求める保全手段の相当性（4 号）も説明する必要があります。

(ii) 効果

申立てが認められた場合の保全手続は、技術関連の営業秘密侵害事件の場合、現地調査の書面記録、作図、撮影、録音、録画、設計と製造図面の複製等の保全措置を講じることができます（第 12 条)。より具体的には、申立ての内容や営業秘密の内容にもよりますが、例えば、被疑侵害営業秘密がある製品の製造方法である場合、裁判官が被告の工場に赴き、工場内でその製品の製造ラインの静止

画を撮影したり、実際に当該製品を製造する工程を動画撮影したり、製造工程表などの収集が試みられることになると考えられます。

証拠保全には強制力がなく、被告側が工場内への立ち入りを拒否することも少なくありません。しかし、当事者が正当な理由なく証拠保全への協力を拒否するかまたは証拠保全を妨害し、証拠の保全ができなくなった場合、人民法院は、その当事者が不利な結果を負うことを確定することができます（13 条）。また、人民法院が保全措置を講じた証拠について、当事者が勝手に証拠の実物の解体・取替え、証拠資料の改ざんまたはその他の証拠破壊の行為を実施することにより、証拠が使用できなくなった場合、人民法院は、その当事者が不利な結果を負担することを確定することができます（14 条）。

（3）裁判における秘密保護に関する制度

民事訴訟の審理は公開法廷で行われるのが原則ですが、営業秘密関連事件については、当事者の申立てにより、非公開審理とすることができます（民事訴訟法 137 条）。このほか、司法解釈には、民事訴訟手続きにおける秘密保護措置について、以下のような規定があります（「最高人民法院による営業秘密侵害民事事件の審理における法律適用の若干問題に関する規定」法釈〔2020〕7 号第 21 条）。

当事者又は訴外人の営業秘密に係る証拠、資料について、当事者又は訴外人が人民法院に書面で秘密保護措置を講じることを申し立てた場合、人民法院は、保全、証拠交換、証拠調べ、鑑定委託、尋問、法廷審理等の訴訟活動において必要な秘密保護措置を講じなければならない。 前項にいう秘密保護措置の要求に違反して、営業秘密を無断で開示した場合、又は訴訟中に接触、獲得した営業秘密を訴訟活動以外で使用若しくは他人にその使用を許諾した場合、法に基づいて民事責任を負わなければならない。民事訴訟法第百十一条[13]に定める事由に該当する場合には、人民法院は、法に基

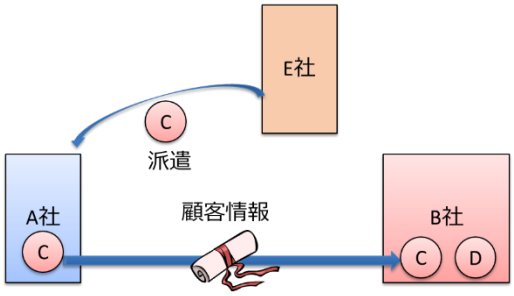
[13] 2021 年改正前の民事訴訟法 111 条の規定であり、執筆時点で有効な民事訴訟法における対応規定 114 条には、例えば、暴力等の手段により司法職員の業務執行を妨害した場合等において、人民法院は罰金等を科すことができる旨、規定されています。

づいて強制措置を講じることができる。犯罪を構成した場合、法により刑事責任を追及する。

このように、秘密保護措置には、日本の不正当競争防止法上の秘密保持命令に相当する措置も含まれています。

6．営業秘密に関する紛争・事件―参考裁判例

（1）顧客リスト等の流用事案において、秘密保持契約の規定内容を理由に管理性が否定された事例

基本情報	裁判所／審級	北京市朝陽区人民法院／一審[14]
	事件番号	（2019）京 0105 民初 11676 号
	判決年月日	2020 年 12 月 30 日
	一審原告	A 社
	一審被告	B 社
		C、D（いずれも個人）
経緯	 ・A 社は、機械設備の製造等を行う外国企業の中国法人であり、中国における販売代理業務や、製品のアフターサービス等のカスタマーサービスを行っていた。	

[14] 本件は営業秘密侵害以外の不正競争行為も訴訟物となっており、一審被告によりこれについてのみ上訴されたため、ここでは一審判決の番号等を記載しました。

	・2012 年及び 2014 年、C は、人材派遣会社（訴外 E 社）との間で、C を A 社に派遣する旨の労働契約を締結し、あわせて、E 社及び派遣先の営業秘密を漏えいしたり、不正に利用しない旨を約定した。C は A 社において、エンジニアとして、顧客のテクニカルサポート等の業務を担当した。 ・2015 年、上記 C の派遣契約は合意により解除された。C が提出した「退職引き継ぎ書」には A 社の顧客情報が記載されており、顧客の連絡先、連絡先電話番号、顧客の現在の状況、購入予定の設備、顧客の連絡先、A 社製品に対する態度、具体的な製品購入意向などの注意事項が記載された添付資料が含まれていた。 ・また、C の退職に際して、A 社-C-E 社の三者間で締結された契約書には、派遣先の営業秘密を第三者に漏えいしてはならない旨の規定があった。 ・C は、上記派遣契約の締結よりも前に、D とともに F 社を設立。その経営範囲は、電機製品、バルブ研磨機等を含んでいた。 ・上記派遣契約の終了の約 3 か月前、B 社が設立。その経営範囲は、電機設備、バルブ研磨機組立販売等を含んでおり、投資、経営には C、D が関わっていた。 ・A 社は、同社の顧客リスト等の営業秘密が、派遣当時、顧客サービスに関わっていた C を通じて B 社に使用されたとして、B 社、C、D を提訴。
裁判所の認定	・裁判所は、「退職引き継ぎ書」の添付資料について、次のように判示して、非公知性と価値性を認めた。 「顧客名称、連絡先氏名、携帯電話番号、役職、分業体制、A 社製品に対する姿勢、前回のプロジェクトの進捗状況など、また、明確かつ具体的な購入意向も含まれており、これらの情報は、公開ルートを通じて得られる情報とは区別され、詳細な情報の集合体を形成しており、その属する分野の関係者に一般的に知られておらず、容易に入手可能もなく、秘密性を有する。また、当該情報は権利者に競争優位性をもたらすことができ、A 社は上記の情報を蓄積し、人的、物的、経済的リソースを投入しているはずであり、当該情報を保有することにより、製品の販路を開拓し、製品の安定的な販売を維持し、同業界における競争優位性を形成することができる。」

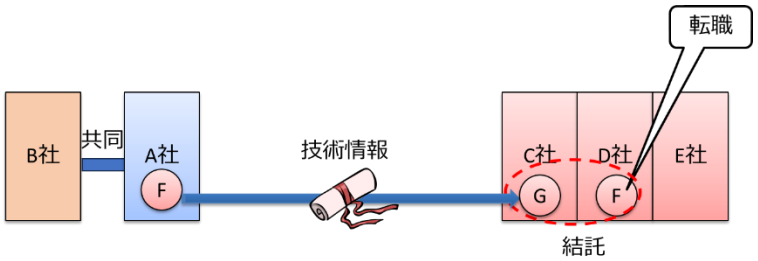
	・しかし、続けて次のように判示して、管理性要件を満たしていないと認定した。 「A 社は C と秘密保持契約を締結していない。 派遣会社の E 社と C の労働契約における秘密保持条項及び A 社-C-E 社が締結した契約には、C が営業秘密を漏えいしない旨の規定があるが、**営業秘密の内容及び範囲は、上記いずれの契約にも規定されておらず**、また、A 社が C に告知したと証明するに足る証拠もないから、A 社の上記顧客情報の管理は、相応の秘密保護措置を欠いている。」

✎ポイント

- 本件は、従業員漏えい型の一種で、派遣社員が競合会社を設立したパターンです。
- 営業秘密に接するのは正社員に限らない以上、従業員からの漏えいも、正社員だけでなく、派遣社員、アルバイト等、労務形態を問わず、人的管理を考えなければならなりません。
- 判示からすると、派遣社員の秘密保持義務は、派遣会社任せにせず、自社でも別途、直接秘密保持義務を課すことが望ましいといえるでしょう。
- 本件では、顧客リストについて、営業秘密の内容及び範囲が秘密保持規定において明確化されていないことを理由に、秘密管理性が否定されました。顧客リスト等の顧客情報が営業秘密に該当し得ることは、派遣社員にも容易に理解可能とも思われるのですが、派遣社員との秘密保持契約でも、できる限り具体的に秘密情報の内容を規定しておくべきでしょう。

（2）発覚から複数回の民事訴訟や刑事手続きを経て、10 年以上の期間を要した従業員漏洩型の事例－バニリン事件

基本情報	裁判所／審級	最高人民法院／二審
	事件番号	（2020）最高法知民終 1667 号
	判決年月日	2021 年 2 月 19 日
	一審原告	A 社、B 社

	一審	C 社、D 社、E 社
	被告	F、G（いずれも個人）
経緯	 ・A 社は、バニラ香料の主原料であるバニリンの製造メーカであり、B 社と共同でバニリンの製造方法を研究開発し、バニリンの世界シェアの約 6 割を占めていた。 ・F は 1991 年に A 社に入社した元従業員であり、2008 年からはバニリン工場の副主任として、バニリンの製造設備のメンテナンス等の業務を担当していた。 ・C 社は食品添加物のソルビン酸塩の研究開発、生産等を行う企業であり、G はその役員である。また、D 社、E 社は C 社の関連会社である。 ・F は、訴外 H 他 1 名とともに、2010 年、バニリン生産技術の提携について C 社及び G と協議し、F らがバニリン製造技術の提供を行うこと等について合意した。F らは、バニリン製造設備図面約 200 点等を含む技術資料が保存された USB メモリを C 社に提供し、その直後に A 社を退職して D 社に入社した。 ・C 社は 2011 年からバニリンの生産を開始し、その後、バニリンの世界シェアの約 1 割を占めるまでになった。 ・2016 年、A 社は、発明者 G・出願人が D 社である、バニリンの生産方法に係る特許出願が、A 社の営業秘密を侵害するものであるとして、D 社と F、G を提訴したが、その二審期間中、訴外 H が USB メモリ、バニリン製造設備図、バニリン提携に係る契約等を公安に提出したため、当該民事事件は刑事事件として公安に移送されることとなった。 ・刑事捜査の過程では、上記 D 社の特許出願は、A 社の独自方法のポイントが含まれていることや、多数の A 社の製造設備図面が、訴外 H が公安に提出した設備図面と同一である旨の鑑定結果が出された。 ・その後、2018 年に、A 社・B 社は、C 乃至 F に対し、営業秘密侵害を理由に民事訴訟を提起。 ・一審裁判所は、差止と 350 万元の損害賠償を認めた。 ・A 社・B 社及び C 乃至 F がいずれも上訴。	

裁判所の認定	・本件の争点は多岐にわたるが、主要な争点についての最高人民法院の判断は以下のとおりである。 ・管理性要件について、裁判所は、以下の事実に基づき、本件技術情報の価値に相応する秘密保護措置が講じられており、管理性要件を充足していると認めた。 ①A 社における管理 ➢ 文書管理手順、記録管理手順などの管理のための文書を整備し、**文書の配布、回収について管理とコントロールを行う**など、会社の重要文書、設備について管理を行った。 ➢ さらに、**研修等を通じて、従業員に対して秘密保持の意思を表示**し、秘密保護措置を講じた。 ➢ 技術情報について、具体的には、B 社との間で秘密保持条項を含む技術開発契約を締結し、「ファイル及び情報管理セキュリティ秘密保護制度」等の管理規定を整備し、職員に対して複数回、秘密保持の広報と教育、研修を行った。 ➢ F は開廷審理の際、漏えいされた**図面が専門部門で保管され、容易に取得できない**と述べている。 ②B 社における管理について ➢ B 社の管理規定には秘密保持に関する規定があり、従業員との労働契約にも秘密保持条項がある。B社は自ら生産は行っておらず、第三者に秘密情報を開示したとの証拠はないから、B 社の措置は合理的かつ有効である。 ・本件には、2019 年改正前の法律が適用されたが、F の営業秘密侵害行為について、裁判所は、F が A 社の営業秘密に接触できたことや、C 社が使用した技術情報とが実質的に同一に同一であることに基づき、F の営業秘密侵害行為（不正取得、開示、他人への使用許諾）を認定した。 ・まず、営業秘密の実質的同一性については、A 社の設備図面と C 社の**設備図面では、構造型式、寸法、設計パラメータ、製造要求等が同一**であり、設備名称と番号、図面番号等も同一であること、また、**工程フロー図については、設備位置と接続関係、材料と媒材の接続関係、制御内容やパラメータ等が同一**であり、一部の図面では図面名称、プロジェクト名称等も同一であったことに基づき、A 社の営業秘密と C 社らが使用した技術情報とが実質的に同一であると認定された。

	・また、F の営業秘密侵害行為に関して、本件では、A 社が要求した秘密保持契約の締結を F が拒否したという事情があったが、裁判所は以下のように判示している：拒否の理由は、退職予定だったからであり、これは署名を拒否する正当な理由ではないし、その後、D 社に入社したことから、F は故意に拒否したと認定できる。F は A 社の上記のような秘密保護措置を知っていたか、知りうべきであった。従業員が在職中に合法的に習得した一般的な知識や技能とは異なり、紙媒体であれ、電子であれ、図面に含まれる技術秘密は A 社の財産であり、その同意がない限り、F は、取得、開示、使用、使用許諾する権利を有しない。 ・損害賠償額について、本件では、C 社ら被告 3 法人が関連帳簿等の提出を拒否したため、裁判所は A 社のバニリンの販売価格と販売利益に基づき、2011 年~2017 年の侵害期間 6 年間の C 社らのバニリン生産量を乗じた上で、さらに、侵害行為の悪質性等を考慮し、1.59 億元の損害賠償額を認定した。

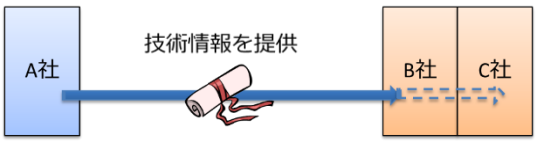
ポイント

- 本件は、判決当時、中国裁判所最高額の損害賠償金が認められた事例として、中国国内で大きな話題となりましたが、発覚から本件二審判決まで、複数回の民事訴訟と刑事手続を経て、紛争の一応の解決まで 10 年以上の歳月を要しました。
- 本件は、従業員漏えい型の一種で、15 年以上在職し、それなりの職位にあった従業員が、競合企業に営業秘密の提供を持ち掛け、在職中に取得して提供、その後、転職した事案です。このように、**退職直前に営業秘密が持ち出されることも多いため、退職の動きが見られた場合には、職務内容に応じてどのような営業秘密に接触していたかも考慮の上、当該従業員への監視を強化**することも考える必要があります。本件のように、秘密保持契約へのサインを拒否したという事情があればなおさらです。
- 本件では、競合企業への営業秘密提供を共謀した者が公安に証拠を提供した点は大きかったと思われ、このような事情がなければ、**証拠保全等の手段の利用を検討する**必要があったと考えられます。
- なお、これまでは、当事者が証拠を収集することが困難であったため、先に刑事摘発を利用し、その結果をもって民事訴訟で損害賠償請求する、というパターンがしばしば見られましたが、本件では逆に、先の刑事摘発は奏功せ

ず、本件二審判決後に改めて公安に移送されることとなりました。

- 本件では、元従業員が秘密保持契約へのサインを拒否したという事情がありました。このようなケースは中国ではしばしば発生していますが、本判例によると、サイン拒否に正当な理由がなく、また、企業が十分な秘密保護措置を講じており、従業員にも周知していれば、そのこと自体はそれほど問題にはならないと思われます。ただし、第Ⅲ章で説明するように、社内規程に会社との秘密保持契約の締結を規定しておくとともに、予め秘密保持契約の締結について、入社時等に承諾を得ておくこと、また、後のトラブルに備えて、サイン拒否された場合には、企業側がサインを要求した事実は証拠化しておくことが望ましいと考えられます。
- 本件では、USB メモリを用いて、営業秘密である図面が持ち出されました。改めて、USB メモリの物理的な使用制限や、図面の管理（専用システム上でのみ閲覧でき、ローカル保存できないようにする等）の措置を検討したいところです。

（3）取引先漏えい型の事例

<table>
<tr><td rowspan="5">基本情報</td><td>裁判所／審級</td><td>最高人民法院／第二審</td></tr>
<tr><td>事件番号</td><td>（2020）最高法知民終 621 号</td></tr>
<tr><td>判決年月日</td><td>2021 年 12 月 18 日</td></tr>
<tr><td>一審原告</td><td>A 社</td></tr>
<tr><td rowspan="2">一審被告</td><td>B 社</td></tr>
<tr><td>C 社</td></tr>
<tr><td>経緯</td><td colspan="2"> 

・A 社は、飼料用添加剤の研究開発、製造、販売等を主な業務とし、塩酸グアニジン-クロロ酢酸法の特許権を有するとともに、グリシン-モノシアナミド法に係る営業秘密を有していた。</td></tr>
</table>

	・2010 年、A 社は、B 社との間で、グアニジン酢酸に関する業務提携契約と、飼料用のグアニジン酢酸製品の生産を B 社に委託する旨の委託契約を締結し、生産設備や用地等を提供することとされた。同契約では、B 社は A 社のグアニジン酢酸の生産技術を厳重に管理し、第三者に売却してはならないこと、そうでなければ A 社に損害賠償する旨、規定されていた。なお、契約及び秘密保持期間は提携終了後 3 年とされた。 ・2012 年、上記提携関係に基づき、A 社は B 社に対し、製造技術を提供したが、2014 年、A 社と B 社の提携関係は終了した。 ・2016 年、A 社は、B 社の関連会社である C 社が、その飼料用グアニジン酢酸を販売、宣伝する際、生産工程が A 社、B 社に由来するものであると公言しているのを発見した。また、C 社が製造した製品の分析報告書からは、A 社の独自製法を利用して製造されたことが疑われた。 ・A 社は、営業秘密侵害を理由に、B 社、C 社を提訴。 ・一審裁判所は、B 社、C 社の行為は A 社の営業秘密の使用と開示に当たると判断し、両被告に対して、侵害行為の停止と損害賠償を命じた。これに対して両被告が上訴。
裁判所の認定	本件の争点は多岐にわたるが、主要な争点についての最高人民法院の判断は以下のとおりである。 ・管理性要件について、裁判所は、以下の事実に基づき、管理性要件の充足を認めた。 ①本件技術情報に接触できる従業員との秘密保持契約書には、以下のような職員の秘密保持義務が明確に定められている。 ➢ 会社が定めた各種の明文又は黙示の秘密保持規定、制度の遵守と役職に対応する秘密保持義務を履行すべき旨 ➢ 会社が保有又は会社が秘密保持義務を有する他社の技術情報その他の営業秘密情報を第三者に漏えい、公開、発表、出版、譲渡その他の方法で知られてはならない旨 ➢ 業務上の必要やその他の理由で役職から離れるか退職する場合、接触した全ての会社の営業秘密関連文書、記録、メモ、データ、プログラムリスト、フロッピーディスクその他の形態の資料は全て会社に返還する旨 ②また、業務提携契約、加工委託契約では以下のような規定がある。 ➢ B 社がグアニジン酢酸の生産技術を厳格に管理し、関連技術の漏えいを防止しなければならない旨

	➢ B 社又はその従業員が関連技術を漏えいし、A 社に損害をもたらした場合にはそれを賠償すべき旨 また、最高人民法院は、次のように判示して、提携契約及び委託契約上の秘密保持期間の終了後における B 社の行為も、「取り決めまたは権利者の営業秘密保守に関する要求に違反して有している営業秘密を開示、使用し、或いは他人に使用を許諾すること。」（※2019 年改正前の規定）[15]の営業秘密侵害行為に該当すると判断した。 「技術ライセンス契約の性質上、ライセンシーは関連する営業秘密を使用する権利を取得するに過ぎず、契約で規定された秘密保持期間は、その満了後、譲受人及びライセンシーが営業秘密を他人に対し、使用又は開示を許可できると解釈すべきではない。 技術ライセンス契約において、ライセンシーは少なくとも次の秘密保持義務を負う：ライセンサーの同意なく第三者に営業秘密の秘密の使用を許可しない／契約規定に基づき秘密保持措置を講じる／故意または過失により営業秘密を開示しない／ライセンサーから提供または教示された技術および関連技術資料については、契約規定の範囲および期間に従い、秘密保持義務を負う／契約規定の範囲および期間を超えてなお秘密保持が必要な技術については、信義誠実の原則に従い、契約に付随する秘密保持義務を履行する。」 裁判所は、以上を踏まえ、C 社の行為も、B 社の違法行為を知りながら A 社の営業秘密を使用した、営業秘密侵害行為に該当すると認定した。

✎ポイント

- 本件では、元ライセンシーの秘密保持義務が課された期間の満了後においても、信義則に基づき、秘密保持義務を負い、これに反する行為は営業秘密侵害に該当すると判断されました。
- 本件は、取引先漏洩型の事案であり、権利者の従業員はこれに関与していませんが、**秘密管理性の認定においては、ライセンス契約における秘密保持規定のみならず、権利者の社内の従業員に対する秘密保持契約の内容等が考慮**されているため、注意が必要です。
- 本件では、約定された秘密保持期間満了後も、ライセンシーは秘密保持義務

[15] 本件は、現行の反不正当競争法の第 9 条第 1 項第 4 号の規定に相当します。

を負うと認定されましたが、そもそも、本件においては、当該技術の重要性や価値寿命との関係において、当初約定された秘密保持期間（3 年間）が適当であったか、疑問が残ります。実務上は、契約終了後も最低 5 年間、又は期間制限なく秘密保持条項が存続する旨の契約も多いです。

- 提携関係終了後に、許諾内容を無断で使用し続けるというケースは、中国においては、営業秘密に限らず、商標権ライセンスやキャラクター著作権ライセンス、販売代理店契約等、様々な類型でよく発生しています。契約終了後の取扱い等について契約で詳細に規定する、または、終了後の相手方の監視等を検討することが望ましいといえます。
- 本件では、B 社・C 社による営業秘密侵害の決め手となった証拠は、B 社が作成した「モノシアナミド法によるグアニジン酢酸の製造」と題するグアニジン酢酸の製造方法が記載された書面です。A 社がこれをどのように入手できたのか、判決には明確な記載がないため、詳細は不明ですが、A 社の子会社が B 社から当該製品を購入する際に入手したようです。製品の売買の際に、製造方法まで詳細に説明する必要はなく（この点は、自社が製品を販売する際にも十分な注意が必要です。）、本件のようなケースは稀であり、通常は、営業秘密侵害の証拠の取得は容易ではないと考えなければなりません。

第３章　漏えい対策実践編

本章のポイント

- 営業秘密を保護するためには、法律上の管理性要件を満たすことが必要であるが、実際に漏えいを防止するためには、物理的管理、人的管理のそれぞれについて、様々な対策を積み重ねて講じる必要がある。
- 具体的な対応ステップは、①セルフチェックシートを用いた現状把握、②秘密情報の洗い出しと区分、③ステップ①、②に応じた管理体制の構築である
- 物理的な管理体制については、日本の「ハンドブック」が大いに参考になるが、中国の場合、携帯電話と SNS 管理については、特に注意が必要である。
- 万一、漏えいが発生した場合、その兆候をいち早くつかむこと（そのための制度の構築も含む）、証拠散逸前に調査と証拠の収集に着手することが重要である。
- 技術関連の営業秘密の場合、中国では、冒認出願されるケースが目立つので、確認と対応が必要。

１．総論

（１）管理体制の構築を考える上での２つの視点

営業秘密漏えいを防ぐためには、どのような管理体制を構築していくべきなのでしょうか。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ものです。

管理体制を整備する本来の目的は、営業秘密の漏えいをできる限り防止・抑止することです。一方、もし漏えいが発生した場合、民事訴訟を通じた法的救済や刑事制裁等の法的措置を求めるためには、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、前章で説明したように、そのための要件として、権利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）が必要となります。

したがって、管理体制を構築する上では、かかる法律上の秘密管理性要件を充足することを基礎として、さらに、実効的に漏えいを防止・抑止する観点からこれを強化していくという「二段構え」で考えていく必要があるといえます。

（2）秘密管理性要件充足性の観点からの管理体制の構築

管理体制の基礎として、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のかについては、前章でも説明した、司法解釈「最高人民法院による営業秘密侵害民事事件の審理における法律適用の若干問題に関する規定」（法釈〔2020〕7号）の第6条の規定が参考になります。

次の各号に掲げる状況のいずれかに該当し、通常、営業秘密の漏洩を防止するのに十分である場合、人民法院は、権利者が相応の秘密保持措置を講じたと認定しなければならない。

（一）秘密保持合意書を締結したか又は契約において秘密保持義務を取り決めた場合
（二）定款、教育、規則制度、書面告知等の方式により、営業秘密に接し、営業秘密を獲得できる従業員、元従業員、サプライヤー、顧客、訪問者等に対して秘密保持を要請した場合
（三）秘密に係る工場、作業場等の生産経営場所について訪問者を制限したか又は区分管理を行った場合
（四）表示、区分、隔離、暗号化、密封保存、接触又は獲得できる人員範囲の制限等の方式で、営業秘密及びその媒体を区分・管理した場合
（五）営業秘密に接し、営業秘密を獲得できるコンピューター設備、電子装置、ネットワーク設備、保存設備、ソフトウェア等について使用、アクセス、保存、複製の禁止又は制限等の措置を講じた場合
（六）退職する社員に対し、接触又は獲得した営業秘密及びその媒体を登記、返却、消去、廃棄し、引き続き秘密保持義務を履行するよう要請した場合
（七）その他の合理的な秘密保持措置を講じた場合

規定上は、必ずしも上記の全てを実行することは要求されていないのですが、営業秘密は、後述するように、様々な形態で、様々な場所に存在することから、基本的には、上記の（一）から（六）は、全て実行する必要があると考えて良いでしょう。

（3）漏えい対策実効性の観点からの管理体制の構築

上記の司法解釈に列挙される秘密保護措置は、それ自体が営業秘密漏えいを防止する効果を有してはいるものの、法律上、保護を与える最低限の保護措置の最低基準を定めたにすぎず、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ります。それぞれのポイントは、以下のとおりです。

■物理的な管理体制の整備

上記司法解釈からも分かるように、秘密管理性要件の最もベースとなる部分は、日本の不正競争防止法と考え方が変わるわけではなく、漏えい防止を強化するための物理的管理体制、つまり、営業秘密の保管・利用場所、形態に応じた、主に、環境面、技術面からの管理体制の構築の考え方も、基本的には日本と同様に考えて差し支えありません。

なお、日本における、営業秘密の物理的な管理体制の整備については、ハンドブック（及びその簡易版・導入用資料である「ハンドブックのてびき」）に詳しく説明されており、中国における物理的な管理体制の整備に際しても、大変参考になるので、是非参照してください。

その上で、中国における物理的な管理体制の整備を考える上では、特に以下の事項を考慮する必要があります。

- 労働者の流動性が高い中国では、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、狙われやすいといえます。日本と同等、あるいは、それ以上に、管理体制を整備・強化する必要があります。

・ 複数の会社が同一敷地内に立地する工業園区に拠点を有する場合、拠点へのアクセス制限が十分となるよう、注意が必要です（→４（４）参照）。

・ 日本とは比較にならないほど、中国では、携帯電話及び SNS が業務上利用されており、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す（→４（２）④参照）。

・ 物理的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ますが、それらが適切に使用されなかったり、あるいは、その前提としての秘密表記等の基本的な措置がとられていなければ意味がありません。最新システムを導入しただけで安心してしまうことのないよう、緊張感を維持しながら、運用を継続していく必要があります。

■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りますが、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ります。規定すべき具体的な事項については、ここでもやはり、「対社内」、「対社外」のそれぞれ、日本と共通する部分も多いですが、労働契約法等の中国の関係法令等の適用に注意する必要があります。

人的管理体制の整備において、中国で特に注意すべき事項は、以下のとおりです。

・ 日本人と中国人との考え方は、異なるところが多いです。日本への留学経験者も増え、日本人のリスク重視の考え方を十分に理解している中国人も、近年、増えてきてはいるのですが、工員などのような一般職員まで含めた場合、全体的には、やはり、営業秘密保護意識は必ずしも十分ではないと言わざるを得ません。研修を含めた啓発活動が必要です（→４（２）⑥参照）。

・ 特に、競業制限については、労働契約法上の要件に注意が必要です（→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すが、締結した契約上の義務がその通りに履行されているとは限りません。例えば、他企業との提携等により営業秘密を開示することになる場合には、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が望ましいです。また、退職者に競業避止義務を課す場合には、補償金を支払う必要があることから、競業避止義務を課した退職者のその後の足取りを、調査会社を利用するなどして追跡、確認する中国企業も少なくありません。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でしょう。

・ 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す。しかし、上述のとおり、地域的リスクが高い中国で、対応をより強化するのは自然なことであり、むしろ、顧客の中国企業の方が、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ものです。顧客に対して「日本式」の遠慮は危険であるし、実は中国の顧客企業も思うほど気にしていないことも多く、無用と考えても良いでしょう。

2．管理体制整備のステップ１－管理体制の現状の確認

前節において、中国における管理体制整備の基本的な視点について説明しました。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ことにします。

（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す。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、中国拠点では、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ます。

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ります。

（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」です。これは、上述の「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、中国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す。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、ぜひ活用してみてください。

セルフチェックシート

カテゴリ	No.	項目
秘密情報の特定	1	□　保有情報をリスト化している
	2	□　保有情報の区分をし、秘密情報を特定している
	3	□　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	4	□　中国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
	5	□　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）	6	□　秘密の記録媒体に「contorolled copy」等の秘密表示がされている
	7	□　プリンターの利用者記録を確認することができる
	8	□　一般情報との分離して保管し、紙媒体等は鍵付きキャビネットに保管されている
	9	□　持ち出しの際の盗難防止策がとられている

	10	□　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）	11	□　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
	12	□　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
	13	□　工場内では携帯電話を使用できる職員が限られている、もしくは禁止されている
	14	□　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立ち入りを制限している
	15	□　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	16	□　保有する電子データはサーバー上で管理している
	17	□　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
	18	□　従業員の PC にパスワードを設定している
	19	□　チャットアプリの使用を禁止・制限している
	20	□　私物の USB メモリ等記録媒体の利用を禁止・制限している
	21	□　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
	22	□　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	23	□　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
	24	□　雇用契約で営業秘密保持を定めている
	25	□　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）

	26	□　守秘義務に違反した際の懲罰規定が明記されている
	27	□　退職者に対し競業避止義務を定めている
	28	□　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
	29	□　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	30	□　秘密保持契約を締結している
	31	□　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	32	□　秘密度の高いエリアには監視カメラを設置している
	33	□　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	34	□　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

なお、「セルフチェックシート」の名称どおり、まずは自社の管理体制をチェックして頂きたいのですが、子会社などの関連会社はもちろん、取引先の管理体制の確認や管理にも活用することもできるでしょう。

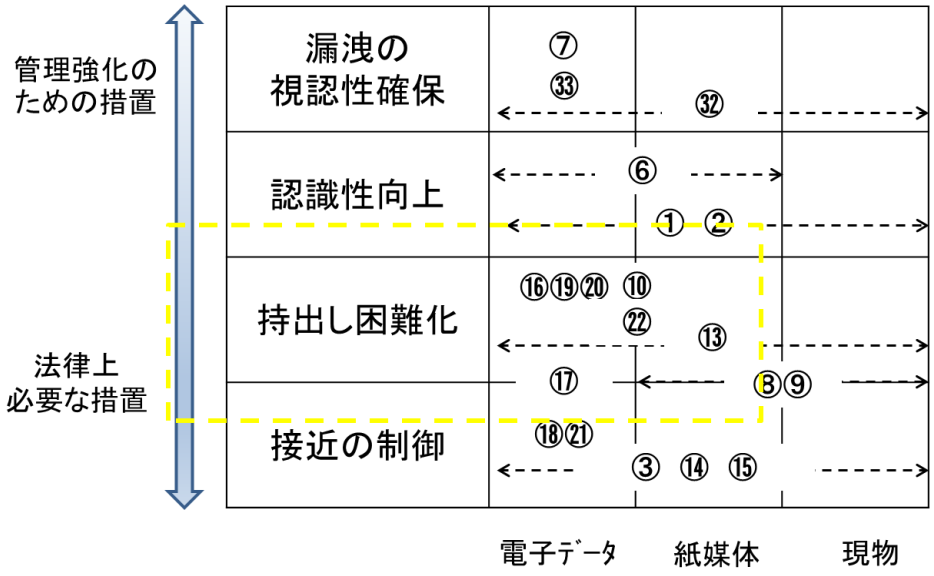
Step Up!

「5つの対策の目的」との関係

ハンドブックでは、営業秘密保護の各対策がどのような効果を有するのかといった目的を意識し、効果的・効率的な対策を選択できるようにするため、秘密情報の漏えい要因を分析し、以下の「５つの対策の目的」として整理しています（☞ハンドブック P22～27）。

i)　接近の制御：秘密情報に近寄りにくくするための対策
ii)　持出し困難化：秘密情報の持ち出しを困難にするための対策
iii）視認性の確保：漏えいが見つかりやすい環境づくりのための対策
iv）秘密情報に対する認識向上：「秘密情報と思わなかった」という事態を招かないための対策
v)　信頼関係の維持・向上等：社員のやる気を高めるための対策

セルフチェックシートの項目 NO.1～33 を上記の i～iv の目的別に分類すると、下図のようになります。



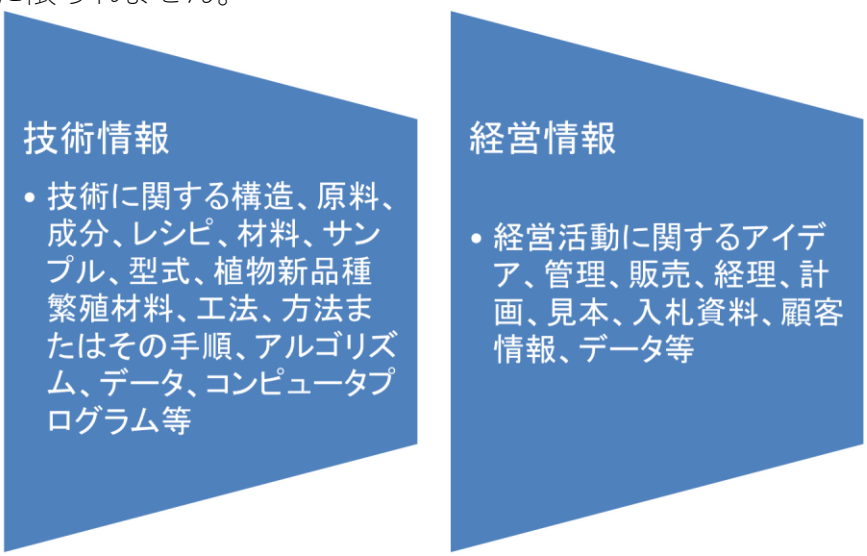
主に、第１節（３）で説明した司法解釈の規定との照合から、法律上必要な措置としてより重要なのは、i）接近の制御と ii）持出しの困難化であり、このためにチェック項目もこの２つに集中しています。

「本マニュアルの使い方」（P.5）では、②ある程度、体制構築が進んでいる状態の企業については、セルフチェックシートで現状の管理体制の「穴」を見つけることを提案していますが、②のタイプの企業の弱点となっているのが、電子データ、紙媒体の持出し困難化に関する措置です。例えば、電子データはサーバで管理していても、ローカルに保存できてしまうケース、印刷物の管理についてのルールがそもそもないというケースが、これまで多く見受けられましたので、このあたりを中心に見直しを行って頂くことをお勧めします。

３．管理体制整備のステップ２－営業秘密情報の洗い出しおよび重要度の区分

（１）営業秘密情報の洗い出し（☞ハンドブック P.10～27）

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します。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良いでしょう。下図は、司法解釈に規定されている、技術情報、経営情報の例です。ただし、司法解釈の規定もあくまで例示であり、また、前章で説明した法律上の定義では、営業秘密は、技術情報、経営情報に限られません。



営業秘密の典型例

Step Up!

顧客リストの営業秘密該当性

中国では、顧客リストの営業秘密該当性については、比較的厳しく判断される傾向があるように思われます。
司法解釈「最高人民法院による営業秘密侵害民事事件の審理における法律適用の若干問題に関する規定」（法釈［2020］7 号）では、「顧客情報」について、**「顧客の名称、住所、連絡先及び取引習慣、意向、内容等の情報を含む。」**と規定されています（1 条 3 項）。

また、同司法解釈施行前の事案ですが、注文日、注文商品名、商品規格、注文数量、連絡先等の情報が記載された顧客リストについて、「一般的なリストであり、顧客の取引習慣、意向及び一般的取引記録と区別されたその他の内容が反映されていない。」として、営業秘密該当性が否定されたケース[16]もあります（なお、顧客情報の営業秘密該当性が認められた例としては、第Ⅱ章の参考裁判例（１）を参照）。

このように、実際の紛争においては、顧客情報の内容によっては、営業秘密として認められない可能性もあります。しかし、上記判例のような顧客リストは、企業にとって価値ある情報であることが多く、一般的には競合他社に知られたくない情報であることには変わりはないから、営業秘密として保護される可能性が全くないわけではないことも念頭に、秘密管理の対象とすべきでしょう。

そして、リスト化の際にポイントとなるが、項目として列挙する秘密情報の「粒度」です。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ります。また、同一の製造工程

[16] (2019)最高法民再 268 号（最高人民法院 2019 年 12 月 16 日判決）

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、電子データとして蓄積されている工程上の管理数値などの電子データでは、管理の具体的な手法は異なってくるので、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と考えられます。

下図は、リストの一例です。例えば、項目は「設計基準書」などのように、部署内の呼称をベースに秘密保持契約よりもさらに具体化し、また、後述する管理規程で情報の重要度や媒体に応じた具体的な管理ルールが定められているのであれば、それと紐づけられるように、各情報の重要度の区分（次の（２）で説明）や媒体を明記すると良いでしょう。なお、営業秘密は日々、新たに発生し得るので、リストは定期的な見直しと更新が必要です。

設計開発部　営業秘密リスト　2023年●月●日更新

No.	カテゴリ	書類／データ名称	媒体	情報区分	アクセス権者	管理方法
1	XX-xx 設計関連資料	設計基準書	電子／紙	極秘	設計開発部全員	・紙資料は中央キャビネットにて施錠管理 ・その他は管理規程●条、●条…に従う
2		性能試験評価データ	電子	極秘	●●課	管理規程●条、●条…に従う
3		設計図面	電子／紙	極秘	●●課	・紙資料は図面室にて施錠管理 ・その他は管理規程●条、●条…に従う
…		・・・	…	…	・・・	・・・

リストの例

いずれにしても、最も重要なのは、も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と思います。

（2）重要度の区分（☞ハンドブック P.17～21）

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また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ありません。したがって、全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ません。

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、重要度別に分類します。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ますが、ハンドブックの該当箇所の記載も参照してください。

４．管理体制整備のステップ３－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.116～128）

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、配置です。中小企業に限らず、大企業であっても、中国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ますが、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、その原因の 1 つとなっているかもしれません。筆者が見てきた限り、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も、中国の製造拠点に配置していない大企業も少なくなかったです。特にコロナ禍以降、地政学的リスクの観点からの対応強化等も相まって、製造業を中心に、本社からの中国駐在員の派遣自体が減ってきているようにも感じられます。

そもそも、日本の本社においても、中国の専利権（特許権等）や商標権を担当する知的財産部員はいても、中国の営業秘密管理を考える担当者は、なかなかいないのではないでしょうか。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ません。いずれにしても、担当者が不在、また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、容易に想定されます。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、中国拠点での指揮、指導を行うのが望ましいかもしれません。

営業秘密管理を担当する専門の部署を設置できれば理想的ですが、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す。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す。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委員会を組織するなどして、定期的に会合の機会を設け、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といえます。

Tips！

専門委員会を設置した大企業／総経理が積極的に指揮を執った中小企業

大企業であれ、中小企業であれ、工場長、総経理（社長に相当）といった組織のトップが関心を持ち、積極的に関わる企業は改善が早いようです。

大企業では、支援事業でのアドバイスを契機に、工場長直轄の専門委員会を設置したケースが複数存在しました。委員会では、全社的な方針の策定や問題点の洗い出しと改善点の討議、各部門の委員から情報共有等の情報共有を行い、工場長が状況を容易に把握できるようにしたほか、委員会で不定期に各部門における秘密情報の管理体制についての内部監査を実施するようにした企業も複数ありました。社内の監査とはいえ、他部門の委員による監査は、相互に緊張感を高め、また、部門内では気づかない問題点や改善アイデアを共有する良い機会となるでしょう。

一方、中小企業の場合、ハンドブック P.116 にも記載されているように、このような委員会的組織まで構成する必要性は高くなく、かえって業務の効率の妨げとなる可能性もあり、あまり推奨されません。しかし、この場合であっても、総経理が自ら各部門の管理体制を確認し、現場の声を聞くなど、経営トップが積極的に問題点の把握に関わる企業は、体制の構築、改善が早いように思われます。
たとえば、ある企業の総経理は、支援事業をきっかけに、初めて各部署の営業秘密管理体制を視察して回りました。その際、社内規程に反して営業秘密に関わる資料をゴミ箱に捨てていた部署の社員の話では、その部署は複数の居室にまたがっており、シュレッダーのある居室は１つしかなく、シュレッダーのない居室では皆、資料はゴミ箱に廃棄しているということだったため、早速シュレッダーを居室ごとに設置するよう、各部門に指示するとともに、その他、Confidential 印や、「立入禁止」プレート、鍵つきキャビネットの購入等の予算を計上することをすぐに決定しました。

企業の規模によって、どのような組織体制とするかは変わりますが、トップがどれだけ関心を持ち、積極的に関与するかは、1つの重要なカギであるように思われました。

（2）従業員の管理

① 対象

正社員はもちろん、工場内で作業を行う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す。派遣社員等については、具体的には、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でしょう。また、第Ⅱ章の参考裁判例（1）を踏まえると、派遣社員個人と直接秘密保持契約を締結することが望ましいといえます。

② 秘密保持契約（☞ハンドブック P.69～71）

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す。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とよいでしょう。従業員との秘密保持契約のポイントは、以下のとおりです（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と良い）
- 中国の一般的な雇用契約に良く見受けられる、「会社の秘密情報を保護しなければならない」といった程度の抽象的な規定では不十分であり、会社が営業秘密として保護しようとする情報の範囲を従業員が知ることができる程度に具体化されている必要がある[17]。
- 契約にて可能な範囲で、秘密情報を列挙、特定しておく（参考書式1、2参照）。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、

[17] (2017)最高法民申 2964 号（最高人民法院 2017 年 9 月 30 日裁定）参照

せっ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よい（下記実例参照）。

- 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。

Tips !

日系企業の管理の実例―営業秘密の分類と取扱いの掲示

A社では、社内の管理規定で、営業秘密情報の印刷物は、不要になった際に、シュレッダー等で復原不可能に廃棄することを義務付け、かかる管理規定は社内に周知されていました。

しかし、実際に執務室内を視察すると、明らかに営業秘密に該当する見積書等の印刷物が、裏紙として再利用されていることが散見されました。現場の中国人社員にヒアリングを行うと、「自分が所属する部署で、具体的に何が営業秘密に該当するか分からない」との声がありました。

各部門において、ある程度、営業秘密及びその取扱いを類型化できると考えられたことから、支援事業においては、各部署にて、一般社員が理解できる粒度にて細分化された一覧を作成し、列挙された各情報について、重要度をランク付けしたり、各情報について、どのような取り扱いが可能／不可能か（例X製品の設計図面：コピー〇、裏紙使用×…等）、が一目でわかるような一覧表を作成し、もし、個別の情報が営業秘密に該当するか、それでも分からない場合には、上司に確認する取り扱いとすることを提案しました。

A社では、部署単位でかかる一覧表を作成して、何が営業秘密に当たるのかを、社員間で共有することにしました。また、特に印刷物の取り扱いに問題があったことから、プリンタ前にこの一覧表を掲示しました。

その結果、各部署で社内の管理規定が実際に守られるようになった、ということです。

③ 競業避止義務／競業避止契約

競業避止義務とは、退職後、特定の期間、特定の地域で、雇用主と競争すること、または、競合他社に務めることを禁止する旨の義務をいいます。中国では、労働契約法上、競業避止義務を課す場合に、以下の要件を満たす必要があります（第 24 条）。

- 高級管理者、高級技術者、秘密保護義務を負担する従業員を対象とすること
- 競業避止義務を課す期間は、2 年以内であること
- 一定の補償金を支払うこと[18]。補償金について約定がない場合、司法解釈（「最高人民法院による労働争議事件の審理における法律適用の若干問題に関する解釈」）には、競業避止義務を履行した労働者は、労働契約解除または終了前の 12 カ月の平均給与の 30%、または、労働契約履行地の最低給与標準額のいずれか高い方の金額に従い、月額補償金の支払いを要求できる旨、規定されている[19]。
- 違約金を規定することもできるが、過大な金額を規定しても、訴訟や仲裁時に限定される可能性がある。

日系企業の場合、競業避止契約のひな型は用意していても、実際に退職者と締結する例はあまり多くないようです。日本では、競業避止義務契約についての法律上の明文規定がなく、その有効性がしばしば問題になることがありますが、中国では、上記のように要件が法律によって定められているとともに、秘密保持契約と異なり、違約金の請求も可能ではあることから、中国企業の方が積極的に活用している印象を受けます。

---

[18] 補償金を支払う必要はないとする見解もありますが、争いになった場合に、補償金の未払いを理由に、裁判所が当該競業避止義務条項を無効と判断されるリスクは否定できません。また、競業避止義務を課された労働者は、補償金が 3 カ月間支払われない場合には、競業避止義務契約の解除を請求できる旨の規定があります（「最高人民法院による労働争議事件の審理における法律適用の問題に関する解釈（一）」（法釈〔2020〕26 号第 38 条）。

[19] 地方の条例において、基準額が定められている場合もあり、おおむね、この司法解釈の基準に沿っていますが、各地の条例内容を確認しておくとよいでしょう。

特に、研究開発に従事していた従業員については、秘密保持契約の締結に加えて競業避止契約を締結することで、秘密保持契約を「補強」し、秘密保持義務の実効性を高める効果が期待できます。

なお、退職時にサインを拒否される可能性もあるため、労働契約等で、退職時に、必要に応じて競業避止義務契約を締結する可能性があることを承諾させておくとよいでしょう。

また、日系企業の場合、競業避止義務契約を締結した場合であっても、企業側は契約に従って補償金を支給するのみで、退職者の義務の履行状況の確認を行うケースはほとんどないと思われます。しかし、違約金のプレッシャーにより当然、契約は守られているものと考えるのは、中国ではやや楽観的にすぎるといえます。この点、中国企業は義務違反の調査まで徹底して行っているように思われます。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ます（参考書式３参照)。

Step Up!

個人情報保護法との関係

中国では、2021 年 1 月から施行されている民法典において、プライバシー権が初めて法律上明記されました（1032 条）。また、同年 11 月からは、個人情報保護法も施行されています。競業避止契約では、契約期間内の現住所、業務状況等についての報告義務を課すことも多いため、プライバシー権及び個人情報保護法との関係が問題となり得ます。
契約の履行に必要な場合には、個人情報の処理についての個人の同意は必要ないとされていますが（個人情報保護法 13 条 1 項 1 号、2 号、2 項）、個別の同意が必要なセンシティブ個人情報（同 29 条）の取得に及ぶ可能性があることを考慮すると、競業避止契約において同意条項を設けた上で、センシティブ個人情報を処理する必要性及び個人の権益に対する影響の告知（同 30 条、17 条 1 項）について、社内のプライバシーポリシー等における告知事項を補完する規定を設けておくのが望ましいと考えられます（参考書式 3 参照）。

また、退職者の義務の履行状況の調査を行う場合にも、個人情報保護法及びプライバシー権との関係が問題となり得ます。
個人情報保護法上、個人情報の処理、収集は、明確かつ合理的な目的と、目的との直接的な関連性を有し、個人の権益に対する影響が最小限の方法で、かつ目的実現のための最小範囲に限られる旨、規定があります（個人情報保護法 6 条参照）。
締結された競業避止契約の履行状況を確認することは、明確かつ合理的な目的と言い得るため、具体的な調査態様がプライバシー権等の権益を侵害せず、目的との関係で最小範囲といえるかが、特に問題となると思われます。

こうした調査とプライバシー権の侵害との関係については、既にいくつか裁判例が存在します。例えば、競業避止義務違反の証拠として、調査委託を受けたコンサルティング会社が元従業員を撮影したビデオの証拠能力が争点の 1 つとなった事案[20]においては、「上記証拠取得はいずれも公共場所で完成しており、（元従業員個人の）プライバシー権及び他人の合法的な権益を侵害する

ことなく、社会公共の利益と社会道徳に反することもない。コンサルティング会社は、証拠取得完了後、当該従業員に係る証拠を流布したり、非合法的な目的、用途に使用したりすることなく、法律が禁止しない特定の範囲内で特定の方式で使用している。」と判示して証拠採用した一審判決が支持されています。
このような裁判例も一定の参考にはなりますが、中国全体として個人情報の保護に対する意識が高まってきていることを踏まえると、かかる調査は、事前に弁護士等に相談し、事案に応じて、収集すべき証拠と適切な調査・証拠収集方法とを確認した上で行うことが推奨されます。

④ 私物携帯電話／ＳＮＳ対策

第Ⅰ章にて説明したとおり、中国では携帯電話（スマートフォン）及び SNS を通じた営業秘密の漏えいリスクが高いことに留意しなければなりません。日本であれば、SNS を業務に利用する例は多くなく、また、勤務時間内に堂々と携帯電話を使用することはためらわれる空気感がありますが、中国では様相が異なります。工場内の動画を SNS に投稿することは日本ではあまり考えにくいことであって、あえて情報管理規程で禁止するという発想自体、なかなか生じないかもしれません。しかし中国では、実際にこうした事例が実際に多く発生していることから、このような当然と思われる事項も、社内規程できちんとルール化し、周知を図る必要があると考えられます。

もっとも、中国では、これらの使用を全面的に禁止することは、多くの日系企業を含む中国企業においては現実的ではないと考えられます。顧客の中国企業の側で、特に WeChat による交信を希望することが多く、また、従業員の強い反発も予想されるからです。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性があるのか－を把握した上で、規制方針と具体的なルールを策定するのが望ましいでしょう。最も厳格な管理を行っている日系企業では、携帯電話の持ち込み自体を禁止している例もありますが、かかる措置が難しい場合には、ある程度の使用を前提としたうえで、どこまでの使用を認めるのか、具体的な統一ルールを社内管理規程にて規定することが考えられます（参考書式 1 参照）。

[20] (2020)皖 02 民終 1096 号（安徽省蕪湖市中級人民法院 2020 年 3 月 30 日判決）

Tips !

日系企業の管理の実例―携帯電話と SNS 管理

(a)工場内での携帯電話の一元管理

Ａ社では、一般的な製造業がそうであるように、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、工場内のそこかしこに秘密情報が存在してる状態でしたが、工場内への携帯電話の持ち込み及び工場内での使用は特に制限されておらず、工場内の営業秘密の携帯電話による漏えいリスクが懸念されました。

ただし、既に携帯電話の使用が常態化している中で、持ち込み自体を禁止することには、従業員からの強い反発が予想され、Ａ社としては、それ以外のやり方で携帯電話リスクを低減したいと考えていました。

そこで、Ａ社に対しては、以下の提案を行いました。

・使用を全面的に禁止するのではなく、例えば、工場内に休憩室を設けてそこで私物の携帯電話を保管し、休憩時間の間のみ、使用を認める
・原則として、工場内での私物の携帯電話による写真・動画の撮影を禁止し、業務上の必要があって、工場内の撮影を行う場合には、会社の共有カメラを用いて撮影する。
・やむを得ず私物の携帯電話等を用いる場合には、撮影の際に、工場内の営業秘密管理担当者等が立会うこととし、また、撮影後は、データは私物の携帯電話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

(b)SNS 利用ルール

Ｂ社では、営業担当者及び生産部門の担当者が、日常的に WeChat を使って顧客の中国企業や社内の他の担当者と連絡を行っており、その中で営業秘密情

報を送受信することもしばしばあり、WeChat からの営業秘密漏えいリスクが懸念されました。

しかし、B社としては、顧客の中国企業が WeChat での連絡を好むため、全面的な使用禁止は取引機会の逸失リスクもあること、また、生産部門においては、夜間にトラブルが発生した場合に、携帯電話で写真を撮影して、WeChat で上司に報告する、という必要性もあったことから、全面的な使用禁止は難しいと考えていました。

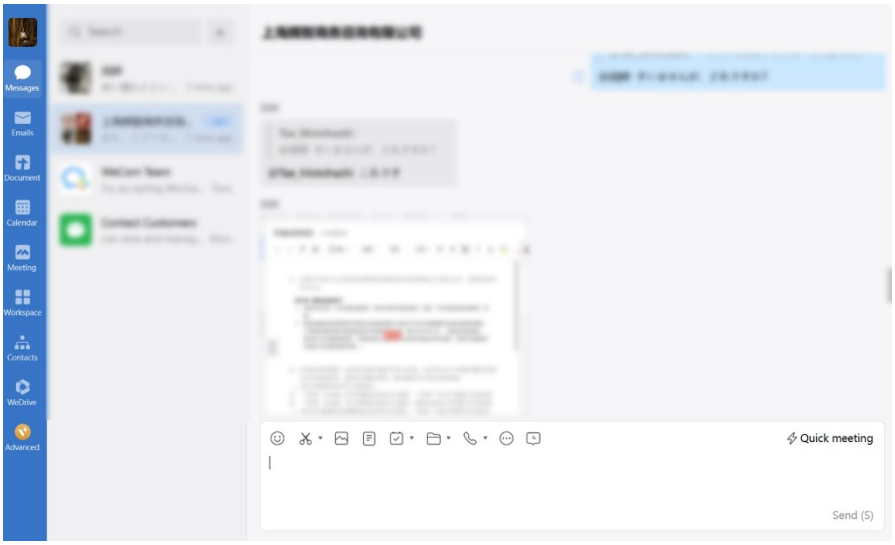
そこで、B社に対しては、以下のようなルールを策定することを提案しました。

・WeChat で送受信できる情報は、営業秘密にかかわらない情報に限定し、営業秘密情報は、上長の事前の許可がない限り、メールでパスワードをかけて送受信すること
・工場内でも、WeChat による営業秘密にかかわる情報の送受信は、原則として禁止する。緊急時には、必要かつ最小限の範囲で、営業秘密にかかわる情報を上長に対して送受信することができるものとするが、その情報が必要なくなった時点で、または、上長の指示に従い、全ての送受信者が当該情報を速やかに削除すること

Step Up!

企業版 WeChat

WeChat には、オフィスユースを想定した企業版 WeChat（「企業微信」）があります。リリースは 2016 年ですが、ここ数年、中国企業を中心に使用されるケースが増えているようです。



企業版 WeChat

企業版 WeChat には、次のような「漏えい対策機能」が設けられています。

・チャット、メール、アプリ内のファイルの操作権限を統一的に管理し、共有ファイルのアクセス制限や、ダウンロードの可否を設定できるほか、ファイルの閲覧、ダウンロード、編集、転送などの挙動を追跡することができる。
・アプリ上で、グループメンバー間で共有されるファイルに、見える電子透かし（複製等防止）と見えない電子透かし（漏えい発生時における漏えい経路の特定が可能）を設定することができる。
・グループ内メンバーのチャットデータに自動暗号化を設定することができ、メンバー以外にチャット内容を知られないようにすることができる。

このように、企業版 WeChat は、特に、社内で情報を共有する際、通常の WeChat を使用するより漏えいリスクの低減の観点から優れていると評価できます。しかし、ユーザーインターフェースは通常の WeChat と同様であり、誤送信等のリスクはあまり変わらないように思われるなど、問題が全くないわけではありません。社内連絡用であっても、共有する情報は極力、秘密情報以外とするのが望ましいでしょう。

なお、WeChat による中国国内外における交信内容が検閲されていることは日本でも広く報道されているところです。
営業秘密の漏えいに加えて、従業員個人の投稿、発信が、会社の見解と受け取られないようにすることにも、あわせて注意する必要があるでしょう。

また、**生成 AI** についても基本的な考え方は SNS 管理と同様です。2023 年、韓国で発生した、従業員の **ChatGPT 利用による営業秘密の漏えい**は、中国でも報道されました。今のところ、中国国内では、生成 AI による営業秘密の漏えい事件は大きく問題となっていないようですが、中国国内の大手企業も相次いで生成 AI サービスをローンチしており、今後、さらに利用、普及が進むことが見込まれるため、企業内でも規制を検討する動きが見られます。**使用の全面的な禁止はやはり現実的ではなく、一定の範囲内での使用を認めつつ、その範囲を社内規程で明確にすること、社員に周知すること、インターネット利用の監視等、複合的な対策を検討する**必要があると考えられます。

なお、2023 年 8 月から「生成人 AI サービス管理暫定弁法」が施行されており、人工知能サービスの提供と使用においては、営業秘密を保護すべき旨の規定が設けられています（第 4 条第 3 号）。

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ので、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ます。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新規ノウハウも、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ですし、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ます。

こうした事態を防ぐため、まずは、労働契約で、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、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いえます。

⑥ 研修（☞ハンドブック P.66~68）

中国は、特許出願件数は、2015 年以降、世界一の座を維持するとともに、知財訴訟の件数も右肩上がりで増加し続けるなど、国全体として見たときに、知的財産権の保護意識は高まってきていると言って差し支えないでしょう。しかし、製造現場で働く社員の一人ひとりにまで、そうした意識が根付いているとまでは言い難いところがあります。したがって、中国における従業員管理においては、従業員の啓蒙活動としての研修も極めて重要です。特に、会社の営業秘密の侵害は犯罪にもなるということ、また、会社の営業秘密を侵害した場合には、損害賠償を請求されたり、懲役刑を受けたりすることを理解させることが、まずは必要でしょう。

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す。

Tips !

日本人との考え方の相違・中国人社員間の意識格差を考慮する

営業秘密の保護に限らず、従業員管理を考える上で、日本人と中国人との考え方の相違を理解しておくことは重要です。一般的に言われることとして、また、実際に中国に駐在した経験を持つ多くの日本人が実感する、日本人と中国人との考え方の大きな相違点が、「日本人は、ものごとの「筋」やルールを重視し、細かいことにもこだわるのに対し、中国人は、目に見える結果・実利を重視し、そこに直結しないことはあまり気にしない」ということです。これを

従業員管理に即して言えば、日本であれば一旦決めたルールは当然、守られるべきものとして受け入れられるのに対し、中国では、決められたルールが必ずしも絶対的なものではなく、自分たちの利益（又は不利益）に直接関係しないのであれば、常に守る必要はないと考えられる傾向がある、ということです。

もちろん、日系企業で働く中国人社員、とりわけ、管理職以上の職員については、日本などへの留学経験もあり、比較的日本人に近い感覚を有し、営業秘密保護及びそのためのルールの遵守の重要性を十分に理解している職員も多いです。しかし、そのような感覚を、例えば、工場で作業を行う全ての社員が共有しているとまでは言いきれないところがあります。第Ⅰ章で紹介した工場内の動画投稿の例はまさにそのことを端的に示しているといえます。自社の工場内の動画を位置情報を付して公開する―これは、要するに、会社の営業秘密を含めて、会社の利益を守るために自分たちが何をしなければならないのか、逆に、何をしてはいけないのかが分かっておらず、そもそも、何が会社の営業秘密であるか、また、営業秘密が会社の財産であることも、おそらくは分かっていない、ということです。

そこで、上述のような、中国人社員間の意識差も踏まえ、管理職と一般従業員とで研修内容を変えること、そして、一般従業員に対しては、実際の営業秘密侵害事件の事例（中国では事欠かない）を紹介しながら、営業秘密は会社の財産であって、その盗用は犯罪行為として罰せられ得ることをまずは理解させ、さらに、営業秘密を保護することは、ひいては自分たちの利益につながることを理解させる内容とすることを推奨しています。

⑦ 退職時の対応（☞ハンドブック P. 75～85）

中国では、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、短期間での転職やジョブホッピングに対しても、労働市場での自己価値の向上と適切な評価を目的とするものとして、比較的ポジティブにとらえられている面があります。こうしたことを背景として、中国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、それだけ高くなるといえます。退職時に営業秘密を全て返還させることはもちろんですが、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したり、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す。

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ますが、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手続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ます。

⑧ 良好な職場環境の整備（☞ハンドブック P.73～74）

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す。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、会社が、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るでしょう。

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すが、社員の長期定着につながり、営業秘密漏えいのためのルールの導入の際に、社員の理解が得られやすくなるという傾向があるように思われます。

Tips !

日系企業の管理の実例―良好な職場環境の整備

(a)地元の若者に「働きたい」と思われる企業を目指す

Ａ社は、某市の郊外に工場を構えています。Ａ社では、ＥＳ[21]を向上させることが、ひいては、会社の競争力向上につながると考えていましたが、近隣には店舗などがなく、中国では一般的な出前なども利用しづらい場所に位置していました。

そこで、Ａ社は、社員食堂を新しく建て替えて、メニューを豊富にしたり、敷地内にコンビニエンスストアを設置したり、社員とその家族が一緒に楽しめるイベントを開催するなど、社員がいかに気持ちよく働けるか、という観点から職場環境の改善を継続的に図りました。

また、Ａ社では、なるべく地元住民を採用することが、従業員の定着につながると考え、地元で開催されるイベント等にスポンサーとして参加するなど、地元の若者に「働きたい」と思われる企業を目指した活動も積極的に行っています。

(b)携帯電話規制ルールをスムーズに導入

Ｂ社では、長期的に見て、ＥＳを高めることが会社の持続的な発展につながると考え、時間をかけてＥＳを重視した種々の取り組みを行ってきました。

そうした地道な取り組みが功を奏し、Ｂ社では高い従業員定着率を維持しています。Ｂ社では、最近、携帯電話の持ち込みを規制するルールを導入したが、導入の際にも、従業員からの反発は特になかった、ということでした。

（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.42～49）

[21] Employee Satisfaction＝従業員満足度のこと。

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る必要があります。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ます。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したほうが良いでしょう。

② 紙資料の管理（☞ハンドブック P.50～51、P.70～71）

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です。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必要があります。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、管理担当者の確認印等）することを検討しても良いでしょう。アクセスへの手間をかけさせることで、おのずとアクセス制限を強化することになるからです。

なお、業種及び部署によっては、特に、製造現場においては、事実上、ペーパーレス化はかなり困難であると思われます。まずは、ステップ２のリスト化の段階で、部署ごとにどのような形態で営業秘密が存在しているのかを把握した上で、実情に即して現実的なルール化を考えることが重要と考えられます。

③ 印刷物の管理（☞ハンドブック P.50～51）

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といえます。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等）についても、社内でルール化しておくと良いでしょう。

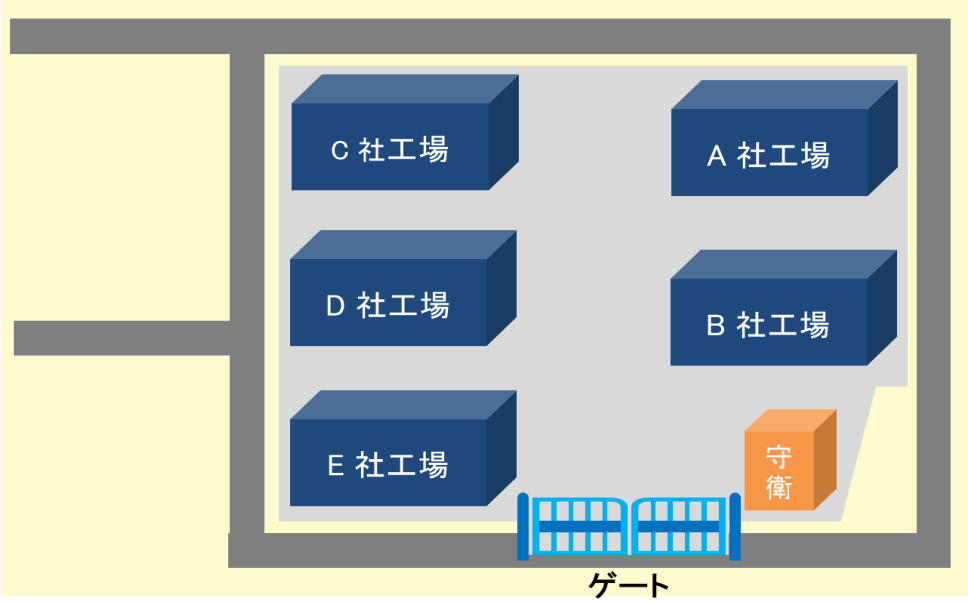
また、裏紙を利用している企業も多いと思われますが、営業秘密保護の観点からは、できれば裏紙利用を禁止したいところです。裏紙利用を認める場合には、上述した「日系企業の管理の実例―営業秘密の分類と取り扱いの掲示」のように、部署単位で具体的に何が営業秘密に該当するか、確実に理解を共有し、営業秘密が裏紙として安易に再利用、廃棄されることを防止する必要があるでしょう。

（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る必要があります。

この点に関連して、「工業園区」にある工場の場合、特に注意が必要となる場合があります。工業園区によっては、高いレベルのセキュリティが確保されている場合がありますが、特に、地方の古くからある工業園区の場合、下図のように、敷地内に複数の会社の工場が、仕切塀などがない状態で隣接して立地しており、部外者が立ち入っても容易に分からない場合も多いです。



工業園区の例

このような場合、工場入り口での物理的なアクセス制限が極めて重要となります。

Tips !

日系企業の管理の実例―工業園区内におけるアクセス制限

(a)工場内にゲートを設置

Ａ社は、某市の郊外の工業園区に工場を有しています。この工業園区の入り口にはゲートがあり、ゲート付近には守衛が配置されてはいましたが、入構の際に身分の確認等は行われておらず、誰でも入構できる状態でした。
また、園区内には、Ａ社のほか、多数の中国企業の工場等が立ち並び、それらの間には仕切塀のようなものはなく、しかも、Ａ社の工場は、開放された入り口からすぐ製造現場となっており、誰でも出入り可能な状態となっていました。

そこで、支援事業においては、Ａ社に対しては、工場の入り口に、施錠可能なドアやゲートを設置すること、受付を設置して、物理的にアクセスを制限するとともに、外部者の立ち入りが分かるようにすることを提案しました。

Ａ社は、工場の入り口付近に受付を設置するとともに、工場の作業エリアの手前に電動ゲートを設置しました。

(b)入館証による管理とオートロックシステムの導入

Ｂ社は、某市の郊外の工業園区に工場を有しています。園区内には、Ｂ社のほか、多数の中国企業の工場等が立ち並び、それらの間には仕切塀のようなものはありませんでしたが、Ｂ社の工場、執務室の入ったオフィス棟のいずれにも、物理的制限がかけられていませんでした。

そこで、Ｂ社に対しては、これらの建物のすべてにアクセス制限をかけること、関係者以外立ち入り禁止の表示をすること、また、誰がいつＢ社を訪問したかが分かるように、入館記録を取ることを提案しました（参考書式７参照）。

Ｂ社は、全建物について、ID カードによるオートロックシステムを順次導入し、工場入り口には「関係者以外立ち入り禁止」の表示を貼付するとともに、総務部門をオフィス棟の入り口付近に移動し、総務部にて来訪者の受付と記録、入館証による管理を行うこととしました。

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ります。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でしょう。

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ますが、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す。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しょう。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ますが、これらの掲示物にも「Confidential」等の表記は必要です。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、または目隠しすることも検討しましょう。

顧客へのアピール、あるいは、従業員の士気を高めるといった目的で、品質改善状況などについて掲示を行っているケースも良く見受けられますが、そうした情報も営業秘密として保護される可能性があることから、これらに営業秘密が含まれていないか、見直しが必要です。

Tips !

日系企業の管理の実例―工場内の掲示物の見直し

A社では、顧客に対する品質アピールのために、工場見学の入り口付近に、品質改善のための取り組み状況や具体的な改善内容などの資料を多数掲示していましたが、中には営業秘密情報が含まれている可能性がありました。

そこで、A社は、全掲示物の見直しを行い、秘密度の高いものは掲示を撤去するとともに、掲示するものについても、写真にぼかしを入れるなどの修正を行いました。

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ります。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、管理を怠りがちです。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る必要があります。

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りえます。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ります。自社内で完全廃棄するのが最も低リスクですが、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ます。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す。

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、廃棄方法を指定したり、監査項目に廃棄状況を含めることも検討すると良いでしょう。

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です。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りますが、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ります。

（5）取引先の管理（☞ハンドブック P.83～97）

① 対象

第１章で述べたとおり、取引先漏えい型の典型は、下請け、顧客企業、ライセンシーなどの業務提携先からの漏えいです。

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、実際には難しくなります。そこで、取引関係に入る前に、資力などの一般的な信用調査を行ったうえ（**経営状態が良くなければ、不払い等の一般的な契約不履行リスクのほか、営業秘密の不正利用のリスクも否定できません。**）で、行政処分歴や訴訟歴もあわせて調査することで、過去のトラブルの有無も確認することが望ましいです。下請けやライセンシーについては、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でしょう。

その他、不良品等の廃棄物処理業者等、営業秘密に接する第三者との間でも、秘密保持義務を課すことが必要です。

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す。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ます。秘密保持条項の主なポイントは、

- 何が秘密情報に当たるかを可能な範囲で特定すること。また、開示する営業秘密に秘密情報である旨の表記をすること。
- 特に、顧客に対しては、不必要に営業秘密を提供することのないよう、予め契約に提供する情報を特定しておく、あるいは、自社が情報提供を断ることができる旨を契約に規定しておくこと（要求された場合に断りやすくなる）を検討する。
- 取引終了時に、秘密情報の返還または破棄（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、下請けやライセンシーに対しては、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（例えば、第Ⅱ章のセルフチェックシートを監査に活用したり、あるいは、別紙として契約内容に含めることも考えられる。）
- 実際の訴訟では、違約金が限定される可能性はあるが、取引先との契約では、

対顧客も含め、違約金規定は、抑止力として、中国でも実務上、よく利用されている。

です。

③ 工場見学

特に、顧客との関係で注意が必要なのが、工場見学です。実際、中国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、**中国顧客企業が、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などの事例が発生**しています。こうした事態を防ぐべく、外部の者の工場見学の際には、以下の対策を検討しましょう。

- 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、秘密保持に関する誓約書を個別に提出させること（→参考書式７参照）
- 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全て預かる**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
- 来訪者の人数にあわせて、複数人で対応し、全来訪者の動きに目が行き届くようにすること

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ますが、むしろ顧客の中国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、遠慮は不要といえます。

④ 共同開発の場合

中国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ます。

この点に関して、最高人民法院（2017）最高法民申 1602 号では、「たとえ一共有者が合理的秘密保護措置をとったとしても、当然に他の共有者が合理的秘密保護措置をとっていたとみなすことはできず、各共有者のいずれもが、秘密情報に対して合理的秘密保護措置をとるべきであると原判決が認定したことは、全く不当ではない」と判示しています。営業秘密の具体的な共有状況にもよると思われますが、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ます。

バニリン事件（第 II 章 6 参考裁判例（2））では、管理性要件の認定において、バニリンの実際の製造を行っていなかった共有者についても、管理性要件を判断しています。この共有者における管理性要件の判断は、実際に製造を行った共有者における管理性要件の判断よりも簡単なものですが、実際の漏えい防止の観点からは、全ての共有者について、営業秘密の重要度に応じて、同等の然るべき措置を講じるべきです。

共同開発前に信用調査等を行うべきこと、秘密保持契約の留意点は、他の取引類型と同様です。

５．漏えい時の対応

（１）漏えいの兆候（☞ハンドブック P.148～150）

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ます（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関わらず）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恐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関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

※中国では、営業秘密漏えい以外の従業員による不正行為もいまだに多く、内部通報制度（☞ハンドブック P.62～63）の活用も視野に入れます。導入されている場合には、内部通報制度を実質的に機能させるための施策（制度の周知、利用の推奨等）を継続的に実施するとともに、通報対象として、セクハラ、パワハラ等イメージがあるかもしれないので、営業秘密漏えいも対象となることを周知しましょう。

※近年、社員へのアンケート調査制度を導入する企業が増えています。かかるアンケート調査は、内部通報のように社員の自主的な行為に依存することなく、会社側からよりフランクに情報を収集することができるというメリットがあります。

※その他、まわりの従業員からの報告・相談が端緒となることも少なくありません。各部署では、日ごろから部下が管理職に相談しやすいような関係性を構築することを心掛けたいところです。

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

※上記のほか、第Ⅱ章６の参考裁判例（２）のバニリン事件のように、退職の際に、秘密保持契約等へのサインを拒否するような場合は要注意です。また、中国では、特に退職（転職）ともに営業秘密が持ち出されるケースが多いことから、上記のような漏えいの兆候の有無にかかわらず、その職位や営業秘密への

アクセス権限の有無、アクセス可能な営業秘密の重要度に応じて、監視を強化することを検討することが望ましいでしょう。

※上記ほか、中国では、WeChat のモーメンツを利用して、被疑侵害品や競業行為の宣伝を行う事例がしばしば見受けられます（(2022)最高法知民終 275 号（最高人民法院 2022 年 11 月 24 日判決）や（2021）滬 01 民終 6208 号（上海市第一中級人民法院 2021 年 7 月 29 日判決））。

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

※中国では取引関係の終了のタイミングで漏えいが発生するケースが多いです。上記のような漏えいの兆候の有無にかかわらず、前節で説明したような秘密情報の確実な返還やその旨の証明書取得等を心掛けましょう。

（２）初動対応(☞ハンドブック P.151～157)

漏えいの兆候が見られた場合、速やかに事実関係を調査・確認すべきです。ここで注意しなければならないのは、中国の知的財産訴訟では、日本と比べて証拠能力が厳格に判断されるため、できる限り、営業秘密侵害に関する証拠を、中国の訴訟実務に即した形で適切に収集することが重要[22]となるところ、内部調査に

[22] 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。

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、ということです。

中国では、特許権等の知的財産権侵害行為に対しては、相手方の侵害行為の実態を調査し、必要な証拠を収集するための専門の調査会社が数多く存在しており、こうした専門の調査会社は、調査対象者に目的をさとられることなく、必要な情報を収集することに慣れています。中国の法律事務所は、自ら、こうした調査会社の機能を有していたり、あるいは、営業秘密侵害を含めた知的財産事件に強みを有する調査会社と提携している例も多いです。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しょう。

とりわけ、2019 年の改正反不正当競争法により新設された、**侵害行為の立証責任転換規定（第 32 条第 2 項）の適用を視野に入れて、初期段階（前述の調査の段階）から、専門家とともに証拠収集方針を決めることは重要**であると考えられます。同条項のうち、1 号と 2 号どちらを選択するかによって、必要な証拠は異なりますが、まずはそれぞれについて、幅広く収集することを検討します**（第Ⅱ章 5(1)(ii)の事例も参照）**。なお、同規定は民事訴訟に適用される規定ですが、後述のように、行政／刑事摘発を利用する場合にも、初歩的な証拠の収集は必要であって、その方針は基本的には重複すると考えられます。

調査を通じて、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（漏洩してしまった秘密情報を含むＰＣやＵＳＢ等の所在、漏洩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す。

以上は主に、侵害行為の調査、証拠収集についての留意点ですが、これと並行して、自社内で営業秘密該当性（特に管理性要件）に関する証拠の収集も行う必要があります（第Ⅱ章 5(１)(i) 参照)。

（３）民事訴訟

① 公証購入

民事訴訟を利用する場合、営業秘密該当性や、相手方の営業秘密侵害行為を証明する証拠を提出する必要があります。民事訴訟に提出する証拠は、原則として

公証認証手続きを経る必要があります。とりわけ、他社が製造、販売している製品について、当該製品が自社の営業秘密を利用して製造されていることを主張しようとする場合、少なくとも、当該製品の公証購入が必要となると考えられます。

「公証購入」とは、被疑侵害品の販売行為等の侵害行為の立証のために被疑侵害品を購入する際、公証人を同行させ、被疑侵害業者による販売行為、販売時に交付された発票などを現認させる手続を指します。かかる公証認証手続なしに被疑侵害品を購入して証拠として提出しても、証拠能力は基本的に認められません。

なお、例えば、侵害された営業秘密が、製品の構成成分とその配合割合であるなど、侵害立証に製品の分析等が必要となる場合、製品を公証購入する前に、サンプル品として購入し、営業秘密との同一性をある程度確認した上で、公証購入を行うことが一般的といえます。

② 証拠保全

また、営業秘密が製法にかかる場合など、公証購入した製品のみからでは、当該営業秘密を使用しているか否かを直接、立証できない場合には、証拠保全制度の利用を検討すべきことになります。

証拠保全制度の概要（要件、効果等）については、第Ⅱ章５（２）を参照してください。証拠保全の申立ての際には、営業秘密侵害の初歩的な証拠として、侵害行為を一定程度推認させる証拠は必要になります。

どのような初歩証拠によって、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、**そうした初歩証拠の所在等も、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しょう。

なお、申立てが認められた場合の保全手続は、申立ての内容にもよりますが、例えば、原告代理人が同行の上、裁判官が被告の工場に赴き、工場内で静止画、動画撮影や、製造プロセス表などの収集が試みられます。

（４）行政摘発

知的財産権侵害についての市場監督管理局による行政摘発は、主に、商標権侵害の場合に利用されることが多く、営業秘密侵害に対する行政摘発は、それらと比べると少ないようです。しかし、行政摘発後に民事訴訟を提起した事例が散見され、これらは主として、営業秘密侵害行為の証拠収集手段として、行政摘発を利用しつつ、民事訴訟で損害賠償を請求したものと考えられます。ただし、行政摘発を行う市場監督管理局は、（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、基本的には、顧客リスト等の経営情報に関する営業秘密侵害の事案について、検討すべきことになるでしょう。

行政摘発は、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すが、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もって、摘発の申立てを行う必要があるため、（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ります。

（５）刑事摘発

刑事摘発も、行政摘発と同様、営業秘密侵害行為の証拠収集手段として利用される場合もあり、刑事罰が課され得る、という点で、侵害者に対する制裁としては、最も重い手段と位置付けられます。刑事摘発の場合も、申立を行うために、侵害にかかる秘密情報の相手方における所在を、調査によってある程度突き止めておく必要があります。

なお、行政機関から刑事移送される場合もあり、これは、基本的には、第Ⅱ章で言及した、刑事訴追基準に関する司法解釈（「最高人民検察院、公安部による公安機関の管轄する刑事事件の立件・訴追基準に関する規定（二）」）に基づき、判断されているようです。

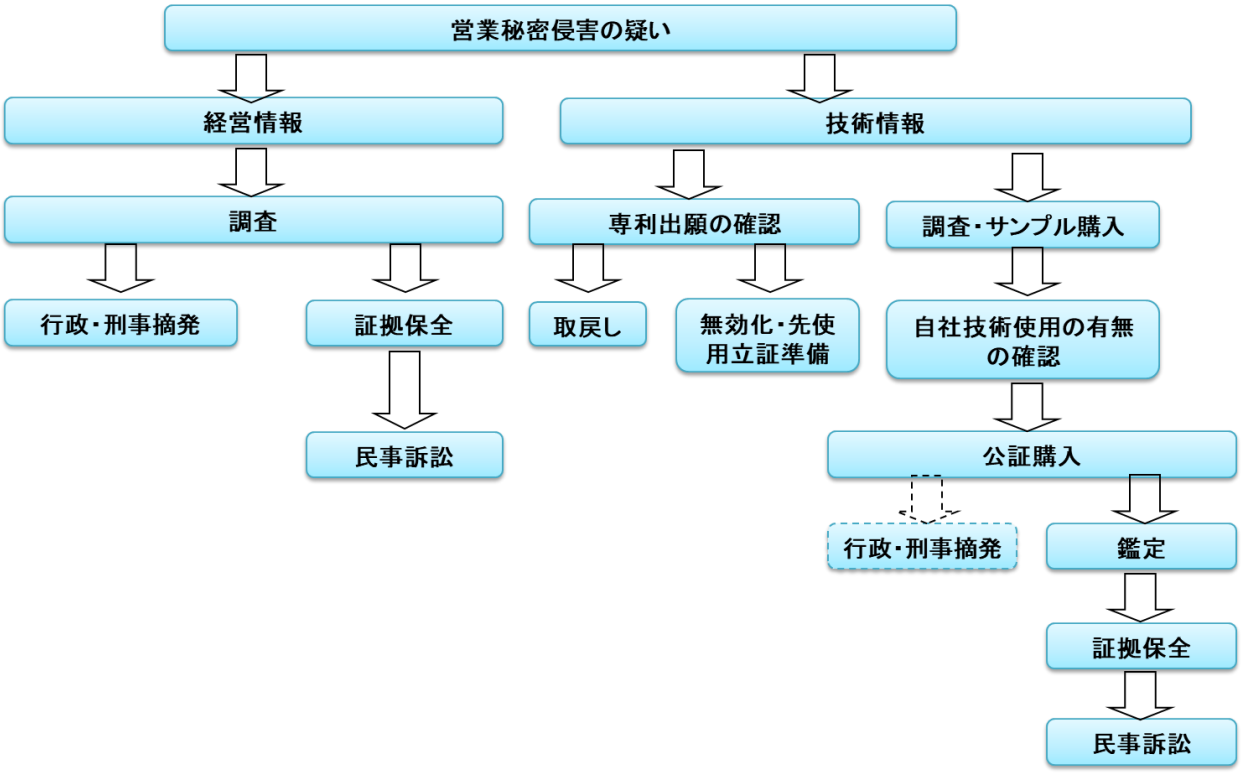
（６）冒認出願の確認

特に、営業秘密が技術情報である場合、第Ⅰ章２で紹介したアスタキサンチン事件のように、中国では、冒認出願されることも少なくありません。このような

冒認出願に対しては、民事訴訟を提起して、権利の取戻しを請求すること、あるいは、無効審判を請求して、権利を無効化することが考えられます。いずれにしても、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ります。なお、冒認権利に基づき、自社また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でしょう。

（7）対応フロー

以上の対応手段をまとめると、下図のようになります。最終的な法的手段の枠組みは、概ね、民事訴訟、行政摘発、刑事摘発のいずれかになりますが、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ってきます。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ります。



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

第〇条 保密规定

1. 员工必须严格保守公司的秘密信息（秘密信息是指，事业企划、产品计划、生产原价、价格决定、客户信息、交易信息、业务合作、技术数据、软件、产品、样品、试作品、图纸、方法等全部有形或无形的经营上的、技术上等的一切商业信息。），事先未经公司书面许可不得向第三者泄露，或用于业务以外的目的。
2. 无论在职时还是离职后，员工都需遵守前款的保秘义务。
3. 员工在离职时，无论离职原因如何，公司可以要求中、高级管理人员（包括但不限于决策成员、重要岗位的管理人员）、关键岗位的操作员工、技术人员以及其他负有保密义务的人员在离职后的 2 年内，不得到与公司生产或者经营同类产品、从事同类业务的有竞争关系的其他用人单位就职，或者自己开业生产或者经营同类产品、从事同类业务。公司将与负有竞业限制的员工签订竞业限制协议，约定相关权利义务。（※１）
4. 未经公司许可，员工不得擅自进入禁止入内的区域，不得因职务范围之外的事由进入不属于自己所在工作区域，或利用公司设备、设施。
5. 使用完样品、图纸、书面资料、带有秘密信息 USB 等机密物品、资料后，应放置于原处，未经许可，不得将与秘密相关的物品、资料带离公司或另作他用。
6. 员工在离职前，应将属于公司资产的电脑、手机等，以及所有的公司资料（包括纸质、电子数据以及保存该数据的所有媒介）返还给公司，或进行删除、销毁，不得保有任何公司资料。
7. 员工在离职后后，不得将公司的顾客或公司的员工带走。
8. 以防止公司秘密信息的泄露，除上述条款外，员工还需要遵守《文书管理规定》、《资讯安全管理规程》等内部规程中的相关规定。
9. 员工因违反上述条款而给公司造成损失时，公司有权追究其赔偿责任。

第〇条　电子邮件、网络等的正确使用

1. 关于公司的电子邮件、以及网络的使用，员工应遵守以下各款规定，使用电脑、手机以及其他通信工具（以下简称，“终端”。），并努力维护正常的网络环境，防止公司的内部信息被损毁或泄露。

（1）　不在业务范围外使用公司提供的终端。

（2）　未经公司许可，不得将自己的终端用于公司业务。

(3)　正确安装、运行并使用公司指定的杀毒软件。

(4)　未经部门负责人同意，不得在公司业务用的终端上下载与公司业务无关的软件，或者可能导致商业秘密泄露的软件。

(5)　未经公司许可，不得将私人的 USB 储存器、硬盘等可以记录信息的媒介或终端连接在公司业务用的终端上。

(6)　前款规定中，员工得到公司许可后进行连接的，应当设置相应密码防止他人擅用。

(7)　进入作业现场前，职工应将终端统一放置于●●处，未经公司许可，禁止使用终端对作业现场、机器等进行拍摄、摄影。

2. 为保证网络的正确使用以及公司秘密信息的管理，在必要时，公司可进行下列事项。

(1)　根据需要，公司可检查下发给员工使用的终端以及保存在服务器中的数据信息，进行分析，并且可以确认员工的网络使用历史信息。

(2)　根据需要，公司可以检查员工收发的公司电子邮件的内容。

(3)　为防止网络病毒，公司有权限制部分网站的访问。

第〇条 物品·设施管理

3. 员工应妥善保管公司的设施、设备、产品、材料、电子化信息、技术信息，未经公司许可不得挪作私用。

第〇条 手机的使用等

1. 个人手机(包括智能手机。下同。)只能在休息室等公司指定的区域内使用。

2. 禁止使用个人手机拍摄公司的秘密信息以及工厂、办公室等公司内部设施、公司设备及机器等(以下称为“秘密信息等”)。但在紧急情况下，可以于必要且最小限度范围内进行拍摄，或在事先得到科长级以上的上级或信息管理负责人许可后进行拍摄。

3. 根据前款的规定进行拍摄后，应将使用完毕的图像数据及时删除。

第〇条 SNS 的使用等

1. 不得使用微信及其他 SNS (Social Networking Service 应用。以下称为“SNS”。)发送或在 SNS 上发布秘密信息等。

2. 虽有前款规定，若出现下述情形，可以在必要且最小限度范围内使用公司指定的 SNS 发送秘密信息等。在此情形，必须充分注意避免因错误发送等引起的秘密信息等的泄漏。

(1) 在制造设备故障、发生事故等紧急情况下，在必要且最小限度范围

内，以向所属部门的上级报告为目的发送秘密信息等的情形。
(2) …
3. 违反前两款规定，发现使用 SNS 收发或在 SNS 上发布公司秘密信息等的，应当立即向所属部门的上级和信息管理负责人报告。

＜参考和訳＞

第〇条 秘密保持
1. 従業員は、会社の秘密情報（秘密情報とは、事業計画、製品計画、生産原価、価格決定、顧客情報、取引情報、業務提携、技術データ、ソフトウェア、製品、サンプル、試作品、図面、方法等、有形無形を問わず、経営上、技術上等の一切の商業情報をいう。）を厳格に保護しなければならず、会社の事前の書面による承諾なく、第三者に開示してはならず、業務外の目的に使用してはならない。
2. 在職中であると離職後であるとにかかわらず、従業員は前項の秘密保持義務を遵守しなければならない。
3. 従業員の離職の際、会社は、離職原因の如何を問わず、中・高級管理職員（会社の決裁者、重要職位の管理職を含むがこれに限らない）、重要職場のオペレータ、技術職員及びその他、秘密保持義務を負う職員に、離職後 2 年以内、会社と同種製品を生産または経営し、同種業務に従事する競争関係にある他の事業主に就職し、並びに、同種製品の生産または経営を自ら開業し、同種業務に従事してはならないことを要求することができる。会社は、競業制限を負う従業員と競業制限契約を締結し、権利義務を約定する。（※１）
4. 従業員は、会社の許可なく、立ち入り禁止区域内に立ち入ってはならず、職務範囲外の事由で自己の所在業務外区域に立ち入り、または、会社の設備、施設を利用してはならない。
5. サンプル、図面、書面資料、秘密情報を有する USB 等の物品、資料の使用後は、もとの場所に戻し、許可なく、機密物品、資料を会社外に持ち出したり、他の用途に使用してはならない。
6. 従業員は、労働契約終了後、会社資産に属するパソコン、携帯電話等およびすべての会社資料（紙媒体、電子データおよび当該データを保存するすべての媒体）を会社に返還し、または削除、破棄しなければならず、いかなる会社資料も保有してはならない。
7. 従業員は、離職後、会社の顧客または会社の従業員を引き抜いてはならない。

8. 会社の秘密情報の漏えいを防止するため、従業員は、上記の条項のほか、さらに、「●●管理規定」等の内部規程中の関連規定を遵守しなければならない。
9. 従業員が上記の条項に違反し、会社に損害をもたらした場合、会社は、その賠償を請求することができる。（※２）

第〇条　電子メール、インターネットの適正な使用
１．会社の電子メールおよびインターネットの使用については、従業員は、以下の各規定を遵守し、パソコン、携帯電話およびその他の通信機器（以下、「端末」という。）を使用し、適切なインターネット環境の維持および会社内部の情報毀損や漏洩の防止に努めなければならない。
(1)　会社が提供した端末を業務範囲外で使用しないこと
(2)　会社の許可なく、自己の端末を会社業務に使用しないこと
(3) 会社が指定したウィルス対策ソフトを適正にインストール、実行すること
(4) 部門責任者の同意なく、会社の業務用端末に会社業務と無関係なソフトや営業秘密漏洩のおそれがあるソフトをインストールしないこと
(5) 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または端末を会社の業務用端末に接続しないこと
(6) 前項の規定において、従業員が会社の許可を得て接続するときは、他人の無断使用を防止するためにパスワードを設定すること
(7) 作業現場に立ち入る前、従業員は端末を●●にまとめて置き、会社の許可なく、端末を使用して作業現場、機器等を撮影することを禁止する
2. インターネットの適正な使用と会社の秘密情報管理を保証するため、会社は次の事項をおこなうことができる
(1) 必要に応じて、会社は従業員に提供した端末及び会社のサーバに保存されるデータを検査し、分析を行い、従業員のインターネット使用履歴情報を確認することができる
(2) 必要に応じて、会社は、従業員が送受信した会社の電子メールの内容を検査することができる
(3) ウィルス感染を防止するため、会社は、特定のホームページへのアクセスを制限することができる

第〇条 物品･施設管理
3. 従業員は会社の施設、設備、製品、材料、電子化情報、技術情報を

適切に管理し、会社の許可なく、私的に使用してはならない

第〇条 携帯電話の使用等

１．私物の携帯電話（スマートフォンを含む。以下同じ。）は、休憩室その他、会社が指定したエリア内でのみ使用できるものとする。

２．私物の携帯電話を用いて、会社の秘密情報、並びに、工場、執務室その他の会社の施設内部、会社の設備及び機器等（以下、「秘密情報等」という。）を撮影することを禁止する。ただし、緊急時において、必要かつ最小限の範囲内で撮影する場合、及び、予め課長クラス以上の上長または情報管理責任者の許可を得て行う場合はこの限りでない。

３．前項の規定に基づき撮影を行った場合においては、不要となった画像データは速やかに消去するものとする。

第〇条 SNS の利用等

１．微信その他の SNS（Social Networking Service アプリケーション。以下、「SNS」という。）を用いて、秘密情報等の送信又は投稿を行ってはならない。

２．前項の規定にかかわらず、以下の場合には、必要かつ最小限の範囲で、会社が指定した SNS を用いて、秘密情報等を送信することができるものとする。この場合においては、誤送信等による秘密情報等の漏えいに十分留意しなければならない。

（１）製造設備の不具合、事故の発生その他の緊急時において、必要かつ最小限の範囲で、所属部門の上長に対して報告する目的で秘密情報等を送信する場合。

（２）・・・

３．前 2 項の規定に違反して、SNS を用いて会社の秘密情報等が送受信又は投稿されていることを発見した場合には、直ちに所属部門の上長及び情報管理責任者に報告しなければならない。

（※１）競業避止契約について、退職時にサインを拒否される可能性を考慮し、予めこのような規定を設けておくことが考えられる。また、労働契約で、会社が競業避止義務を課すことが必要と判断した場合には、競業避止義務契約にサインすることを予め承諾させることも考えられる。

（※２）労働契約法においては、使用者の費用で技術研修を受けさせる場合の服務期間の約定に違反した場合、及び、競業避止の約定に違反した場合を除き、違約金を約定できない旨、規定されている（第 25 条）。

２．従業員との秘密保持契約書の例

保密协议书

甲方：
住所地：
法定代表人：
联系电话：

乙方：
身份证号码：
经常居住地：
户籍所在地：
联系电话：

鉴于：
乙方为甲方员工或为甲方提供劳务，乙方在任职中有接触甲方商业秘密的可能，现根据《中华人民共和国劳动法》、《中华人民共和国反不正当竞争法》等相关法律、法规，双方签订如下的保密协议：

第一条 商业秘密的定义
本协议所称商业秘密，是指甲方固有的，顾客信息、事业计划、企划、know-how、软件、技术数据、产品计划、产品、样品、图纸、方法等全部有形或无形的经营上的、技术上等的一切商业信息。

第二条 保密义务
1、未经甲方同意,乙方不得向第三人披露、泄露甲方商业秘密。
2、乙方不得在履行甲方职务以外使用或变相使用商业秘密。
3、如发现商业秘密被泄露或者因自己过失泄露商业秘密的，乙方应当采取有效措施，以防止泄密进一步扩大，并及时向甲方报告。
4、甲乙双方确认，本条前三款保密义务的期限、以不违反甲方意图为前提、直至相关秘密信息公开时止。乙方是否在职，不影响保密义务的承担。

第三条 商业秘密的返还等
乙方应当于离职时，或者于甲方提出要求时，将自己持有的载有商业秘密的一切载体、资料交还给甲方，不得将这些载体及其复制件擅自保留或交给其他任

何单位或个人。

第四条 损害赔偿
乙方违反前款规定，擅自披露、泄露商业秘密或在职务范围外使用商业秘密的，甲方可惩处乙方。造成损失的，甲方可要求乙方进行赔偿。

第五条 其他约定
1、因本合同而引起的纠纷，双方应协商解决，如果协商不成需诉讼解决的，因本协议而引起的纠纷，双方应协商解决，如果协商不成需诉讼解决的，双方一致同意将纠纷起诉至甲方工商注册地人民法院。（※１）
2、本协议正本一式两份，双方各执一份，自双方签字或盖章之日起生效。

甲方：(公章)
法定代表人签字（盖章）：
日期：

乙方：
签字（盖章）：
日期：

＜参考和訳＞

秘密保持契約書

甲：
所在地：
法定代表者：
電話：

乙：
身分証番号：
住所：
戸籍住所地：
電話：

乙が甲の従業員として、または、甲のために労務を提供し、乙が在職中に甲の営業秘密に接触する可能性があることに鑑み、「中華人民共和国労働法」、「中華人民共和国反不正当競争法」等の関連法律、法規に基づき、双方は以下の秘密保持契約を締結する：

第一条 営業秘密の定義
本契約書にいう営業秘密とは、甲固有の顧客情報、事業計画、プロジェクト、ノウハウ、ソフトウェア、技術データ、製品計画、製品、サンプル、図面、方法等の有形または無形の経営上または技術上等の一切の商業情報をいう。

第二条 秘密保持義務
1、甲の同意なく、乙は甲の営業秘密を第三者に開示、漏えいしてはならない。
2、乙は、営業秘密を、甲の職務の遂行以外で使用または間接的に使用してはならない。
3、営業秘密の漏えいまたは自己の過失によって営業秘密が流出した場合には、乙は有効な措置をとるとともに、営業秘密の流出の拡大を防ぐため、直ちに甲に報告しなければならない
4、甲乙双方は、前３項に規定する秘密保持義務の期限が、関連秘密情報が甲の意に反することなく公開される時まで継続することを確認する。乙が在職中であるか否かは、秘密保持義務の負担に影響しない。

第三条 営業秘密の返還等
乙が離職する際または、甲が提出を要求した場合には、自己が保有する営業秘密が記録された一切の担体、資料を甲に返還するものとし、これらの担体及びその複製物を無断で保持または他のいかなる組織または個人に交付してはならない。

第四条 損害賠償
乙が前条の規定に違反し、営業秘密を無断で開示、漏えいし、または、職務の範囲外で使用した場合には、甲は乙を処分することができる。損害が発生した場合には、甲は乙に賠償を請求することができる。

第五条 その他
1、本契約によって発生した紛争は、双方が協議で解決するものとし、協議

が成立しない場合には、甲の工商登記地の人民法院に提訴することができる。（※１）

2、本契約は一式二部とし、双方が一部ずつ保有し、双方が署名、押印した日から効力を生じる。

甲：（社印）
法定代表者署名（印）：
日付：

乙：
署名（印）：
日付：

（※１）管轄法院（裁判所）を定めておいた方が良い。

３．退職後の競業避止契約書の例

竞业限制协议书

甲方：
住所地：
法定代表人：
联系电话：

乙方：
乙方身份证号码：
乙方经常居住地：

第 1 条 竞业限制范围
鉴于乙方在甲方任职时所获得的知识和经验涉及甲方重要的商业秘密以及 know-how，乙方从甲方离职次日起●年内（※１），未经甲方同意，乙方不得从事下列行为。
1、在与甲方有竞争关系的单位内任职或以任何方式为其服务
2、自己生产、经营与甲方有竞争关系的同类产品或从事同类业务
3、其他提供与甲方同类产品或从事同类业务的行为
此外，乙方作为甲方员工，在任职期间也理所应当的遵循上述的竞业限制义务。

第 2 条 竞业限制期的相关情况通报（※２）
1、乙方应在离职后的每季度结束前的最后十日内，以电子邮件、信件、传真等方式，向甲方法定代表人如实地书面通报其现在的住所地址、联系方法、工作情况、证明人姓名及联系方式，以及甲方要求通报的相关内容。
2、甲方为了确认上述情况，可以就乙方竞业限制义务的履行情况进行必要的确认和调查，并要求乙方就其履行情况进行汇报。
3、为了签订及履行本合同，乙方同意，关于本合同规定的竞业限制期间及可追究本合同违约责任的期间内，甲方可处理（包括收集、使用、存储等）乙方的个人信息及涉及个人隐私的信息（身份证号码、住址、邮政编码、手机号码、电子邮件地址等联系方式、银行账户信息、就业单位名称、业务内容以及其他用于确认竞业限制义务履行情况的信息）。甲乙双方确认，基于本合同处理乙方的个人信息时，甲方应告知乙方的其他事项符合甲方的个人信息保护规则。

第 3 条 竞业限制期的补偿

1、乙方离职后的竞业限制期为●年，自_____年__月__日起至____年__月___日止。

2、补偿方式如下：(※３)

甲方同意给付乙方竞业限制补偿费（____年__月__日前以工资形式发放)，标准为每月●元。补偿费从_____年__月开始，按月支付，由甲方于每月_日前存入如下银行账户内。

开户行：　　，户名：　　，银行账号：　　。

甲方有权按国家及●市有关规定从前述费用中依法扣缴相关税费。

2、竞业限制期满，甲方即停止补偿费的支付。

第 4 条 竞业限制的解除

甲方如认为乙方已无竞业限制必要，有权以通知的方式终止乙方的竞业限制义务。

第 5 条 违约金

乙方违反本合同约定的竞业限制义务的，应向甲方支付【本合同约定的竞业限制期×每月的竞业限制补偿金金额×●倍】的违约金。乙方的违约行为给甲方造成的损失超过该违约金的，甲方可另行向乙方追偿。

第 5 条 争议解决

因本协议发生的或与本协议有关的任何争议，双方应协商解决。协商不成，由甲方工商注册地人民法院管辖并依法判决、裁定。

第 6 条 其他

1、本协议经双方盖章或签字后生效。一式两份，甲乙双方各持一份，具有同等的法律效力。

2、乙方离职后的送达地址为：

地址：　　邮编：

收件人：

联系电话：

乙方变更送达地址应书面通知甲方。

3、本协议如与双方以前的口头或书面协议有抵触，以本协议为准。

本协议的修改必须经双方一致同意并采用书面形式。

甲方：　　（盖章）

年　　月　　日

乙方：　　（签字或盖章）

年　　月　　日

＜参考和訳＞

競業制限契約書

甲：
所在地：
法定代表者：
電話：

乙：
身分証番号：
住所：
戸籍住所地：
電話：

第 1 条 競業制限範囲
乙が甲において在職中に獲得した知識と経験は甲の重要な営業秘密及びノウハウにかかるものであることに鑑み、乙は甲を離職した日から●年以内（※

１)、甲の同意を得ず、以下に掲げる行為に従事することができない。
1、甲と競争関係にある組織内で何らかの職務に就き、または、何らかの方式で労務を提供すること。
2、甲と競争関係を有する同種製品または同種業務について、自ら生産、経営すること
3、その他、甲と同種製品を提供または同種業務に従事する行為
　　また、乙は、甲の従業員として、在職期間中も上記競業制限義務を遵守しなければならない。

第 2 条 競業制限期間の状況通知（※２）
1、乙は、離職後、毎四半期末 10 日以内に、電子メール、書簡、ファクス等の方式で、甲の法定代表者に対し、現在の住所、連絡方法、業務状況、保証人の氏名及び連絡方式、及び甲が通知を要求する関連内容について、事実をそのまま書面で通知しなければならない。
2、甲は、前記の状況確認のため、乙に対し、競業避止義務の履行状況について必要な確認・調査を行い、報告を求めることができる。
3、本契約の締結及び履行のため 、乙は、甲が本契約の規定に関し、競業避止期間及び本契約の違約責任を追及できる期間内において、乙の個人情報及びプライバシーに係る情報（身分証明証番号、住所・郵便番号・携帯電話番号・メールアドレス等の連絡先、銀行口座情報、就職先名業務内容及びその他競業避止義務の履行状況を確認するための情報）を処理（収集、使用及び保存等を含む）することに同意する。甲及び乙は、本契約に基づく乙の個人情報の処理に際して甲が乙に告知すべきその他の事項については、甲における個人情報保護規則に準拠することを確認する。

第 3 条 競業制限期間中の補償
1、乙の離職後の競業制限期間は●年、＿＿年＿月＿日から＿＿年＿月＿＿日までとする。
2、補償は以下のとおり行う：(※３)
　甲は乙に、毎月●元（＿＿年＿月＿日前の給与形式の支払い）を基準として、競業制限の補償金を支払うことに同意する。補償金は、＿＿年＿月から、甲は毎月＿＿日までに以下の銀行口座に振り込み入金する。
　銀行名：　　口座名義：　　口座番号：
　甲は、国家及び●市の関連規定に従い、前記費用から関連税金を控除することができる。
3、競業制限期間満了後、甲は直ちに補償金の支払いを停止する。

第 4 条 競業制限の解除
乙に対する競業制限の必要がなくなったと判断した場合には、甲は、いつでも乙に対し、競業制限義務の終了を通知することができる。

第 5 条 違約金
乙が本契約に規定する競業制限義務に違反した場合には、甲に【本契約に規定する競業制限期間×毎月の競業禁止補償金額×●倍】の違約金を支払う。乙の違約行為が甲に違約金額を超える損害をもたらした場合には、甲は乙に対してさらに賠償を請求することができる。

第 6 条 争議解決
本契約によって発生し、または、本契約と関連するいかなる紛争も、双方の協議により解決するものとする。協議が不成立の場合には、甲の工商登記地の人民法院の管轄で法に基づき裁決する。

第 7 条 その他
1、本契約は双方の署名押印により効力を生じる。一式二部とし、甲乙双方が一部ずつ保管し、それらは同等の法的効力を有する。
2、乙の離職後の送達先は以下のとおりである：
住所：　　郵便番号：
受取人：
電話：
送達地の変更は、書面により甲に通知しなければならない。
3、本契約と、双方が本契約以前の口頭又は書面契約が抵触する場合には、本契約を基準とする。
本契約の修正は、双方の同意した書面形式を採用しなければならない。

甲：　　（社印）

年　　月　　日

乙：　　（署名または印）

年　　月　　日

（※１）最長で２年である（労働契約法第 24 条第２項）

（※２）このように、履行状況を報告させても良い。この場合、報告事項が個人情報保護法上のセンシティブ情報に該当すると考えられるが、センシティブ情報についての告知事項は、以下の 6 つとなる（個人情報保護法第 17 条、第 30 条）。

①個人情報処理者の名称又は氏名及び連絡先。
②個人情報の処理目的、処理方法、処理する個人情報の種類、保存期限。
③個人が本法の規定する権利を行使する方法及び手続。
④法律、行政法規が告知すべきであると規定するその他の事項。
⑤センシティブ個人情報を処理する必要性
⑥個人の権益に対する影響

通常は、上記のうちの多くは社内のプライバシーポリシーに規定されていると思われるため、参考書式３では、上記の②、⑤に対応する規定を設けているが、念のため、各社のプライバシーポリシーを参考にされたい。

（※３）補償金の額については、第Ⅲ章４（２）③を参照

４．取引先との秘密保持契約書の例

保 密 协 议

甲方：
乙方：

本协议中披露保密信息的一方称为“披露方”，接收保密信息的一方称为“接收方”。

鉴于接收方与披露方建立_____业务合作关系（以下简称“本合作”），而披露方将因此向接收方披露本协议定义的保密信息。为保证此类信息不被未经授权地披露、使用，经友好协商，双方就如下条款达成本协议。

第一条 秘密信息的定义

本协议中的“秘密信息”是指，披露方向接收方披露（或提供）的产品、样品、试作品、文件、图纸和资料、专业技术以及其他有形或无形的经营上的、技术上的一切重要信息。但是，如果接收方能证明相关信息属于以下任何一项的，不属于秘密信息。

1. 披露时已为公众知晓的信息或接收方已经保有的信息
2. 披露后，不因归责接收方的事由，为公众知晓的信息
3. 接收方无需承担保密义务从有正当权限的第三人处合法取得的信息
4. 非依据披露信息接收方独自开发的信息

第二条 保密义务

1. 接收方应当指定信息管理人员，并书面通知披露方该信息管理人员的姓名及联系方式。
2. 接收方不得向第三人披露、泄露前条秘密信息。但是，接收方得到披露方事先书面同意的，或就业务上有必要知晓秘密信息的员工，可以向第三人/员工披露秘密信息。此情况下，接收方需要求第三人/员工承担本协议规定的义务，并就第三人/员工的全部行为向披露方承担所有责任。
3. 接收方不得在本合作以外的目的使用或利用秘密信息。
4. 接收方除得到披露方事先书面同意外，不得复印或复制记录有秘密信息的任何书面或媒介。
5. 接收方应尽善良管理人的注意义务严格保管、管理披露方提供的秘密信息。万一秘密信息发生泄露、丢失、失窃、盗用等情况时，会立即书面通知披露方。

6. 接收方因法律法规而有责任开示披露方的秘密信息时，接收方应事前或被相关机关通知后尽快书面通知披露方，尽可能在接到披露方指示后行事。

第三条 秘密信息的返还等

本合作终止的，或披露方要求返还的，接收方根据披露方指示在指定期间内返还或销毁全部秘密信息（包括复印件、复制品），以电子方式或其他无形方式保存的，将其删除。此外，接收方就已返还、销毁的事实向披露方出具书面说明。

第四条 不保证

所有秘密信息披露方按原样提供给接收方，披露方对该秘密信息的完整性、正确性、是否符合目的、有用性不做保证，同时也非不侵害第三人的发明专利权、实用新型专利权、其他任何知识产权和其他权利的明示或暗示的保证。

第五条 **检查**（※１）

1. 为确认接收方的秘密信息的保管、管理情况，披露方可以随时（包括秘密信息提供前）要求由披露方或披露方指定的第三方进入接收方的办公室、工厂等的作业现场进行检查，接收方应予以配合。如发现接收方的保管、管理措施不充分或有缺陷的，披露方可以要求接收方进行整改，接收方应遵从披露方的整改指示。
2. 接收方应让根据本协议第二条第 2 款的规定接受秘密信息披露的第三方同样承担前款义务，确保披露方能对该等第三方进行检查、要求整改。

第六条 违约

接收方、接收方的员工以及根据第二条第 2 款的规定接受秘密信息披露的第三方违反本协议规定任何一项条款的，披露方有权向接收方采取其认为的必要措施，同时，可以对接收方重复要求损害赔偿。

第七条 协议期间

1. 本协议的有效期间至　　年　月　日止。但是，甲乙双方达成一致意见的，可以延长或缩短此期间。
2. 本协议因期限届满或解除而终止的，第二条（保密义务）、第四条（不保证）、第六条（违约）和第八条（管辖法院）的规定，目标事项只要存在的，仍持续有效。

第八条 管辖法院

因本协议产生的纠纷，甲乙双方友好协商解决，协商不成不得不进行诉讼的，由被告所在地法院进行管辖。（※２）

本协议一式二份，甲乙双方签字盖章后，各持一份。

年　月　日

（甲）

（乙）

＜参考和訳＞

秘 密 保 持 契 約 書

甲：
乙：

本契約において、秘密情報を開示する当事者を「開示者」といい、秘密情報の開示を相手方より受ける当事者を「受領者」という。
開示者および受領者が、＿＿＿＿の業務（以下「本業務」とする）を遂行するにあたり、開示者は本契約において定める秘密情報を受領者に開示することに鑑み、開示された情報が事前の承諾を得ることなく、第三者に披露・使用されることを防ぐため、甲乙は友好的な協議のもと、次のとおり契約を締結する。

第１条（秘密情報の定義）

本契約において秘密情報とは、開示者が受領者に開示（又は提供）した製品、サンプル、試作品、書類、図面、資料、ノウハウ及びその他の有体物又は無体物の営業上、技術上の一切の重要情報をいう。ただし、秘密情

報が以下の各号の一に該当することを受領者が証明した場合は、秘密情報より除外する。

(1) 開示された時に既に公知であった情報、または既に受領者が保有していた情報
(2) 開示後、受領者の責によらずに、公知となった情報
(3) 受領者が正当な権限を有する第三者から守秘義務を負うことなく適法に入手した情報
(4) 開示された情報によらずに受領者が独自に開発した情報

第２条（守秘義務等）

１．受領者は、情報取扱管理者を定め、書面により開示者に情報取扱管理者の名前と連絡先を通知するものとする。

２．受領者は前条の秘密情報を、第三者に開示、漏洩してはならない。ただし、開示者から書面による事前承諾を得たとき、又は業務遂行上知る必要のある従業員に限定して、秘密情報を第三者／従業員に開示することができる。この場合、受領者は、当該第三者／従業員に対し本契約で定める義務を課し、その行為全てを受領者の行為として開示者に対して一切の責任を負う。

３．受領者は、秘密情報を委託業務以外の目的のために使用または利用してはならない。

４．受領者は、開示者からの書面による事前承諾を得た場合を除いて、秘密情報を記録したいかなる書面または媒体も、複写または複製してはならない。

５．受領者は、善良なる管理者の注意をもって開示者から取得した秘密情報を管理する。万が一、秘密情報の漏洩、紛失、盗難、盗用などが生じた場合、書面にて直ちに開示者に通知する。

６．受領者は、法令により秘密情報等の開示が義務づけられた場合には、事前に開示者に通知し、開示につき可能な限り開示者の指示に従うものとする。

第３条（秘密情報の返却等）

本契約が終了したとき、または開示者から返却要請があったときは、受領者は開示者の指示に従い、指定された期間内にすべての秘密情報（複写、複製したものがあればそれを含む）を返却または廃棄し、電子的またはその他の無形的形態で保持されているものについては、これを消去するものとする。また、受領者が既に返却、廃棄した事実を書面にて開示者に提示する。

第４条（不保証）

すべての秘密情報は開示者から受領者に現状のままで提供され、開示者は当該秘密情報について、その完全性、正確性、合目的性、有用性等の保証をしないほか、第三者の特許権、実用新案権、その他のいかなる知的財産権およびその他の権利を侵害しないことを明示的または暗示的に保証するものではない。

第５条（監査）（※１）

１．受領者の秘密情報の保管・管理状況を確認するために、開示者はいつでも（秘密情報の披露以前を含む)、開示者自らまたは開示者が指定した第三者をして、受領者の事務所・工場への立ち入り検査することができる。受領者は当該監査に協力する。開示者は、受領者の保管・管理措置が不十分又は欠陥があると判断した場合、受領者に対して是正措置を求めることができ、受領者はこれを実施しなければならない。

２．受領者は、本契約２条２項の規定により営業秘密を受領する第三者に前項と同等の義務を負わせ、開示者が当該第三者に監査・是正措置を求めることができることに承諾する。

第６条（契約違反）

開示者は、受領者、受領者の従業員及び本契約２条２項の規定により営業秘密を受領する第三者が本契約に定める各条項の一に違反した場合、開示者は受領者に必要と認める措置を請求することができる。この場合、開

示者は受領者に対してさらに損害賠償の請求をすることができる。

第７条（契約期間等）

１．本契約の有効期間は●年●月●日までとする。ただし、甲乙間で合意した場合は、この期間を延長または短縮することを妨げない。

２．本契約が満了または解除によって終了した場合でも、第２条（守秘義務等）、第４条（不保証）、第６条（契約違反）および第８条（管轄裁判所）の規定は、対象となる事項が存在する限り、なお有効とする。

第８条（管轄裁判所）

本契約に関し紛争が生じたときは、甲乙友好的に協議し解決するものとするが、やむを得ず訴訟の必要が生じた場合には、被告所在地の裁判所を管轄裁判所とする。（※２）

本契約成立の証として本書２通を作成し、甲乙記名押印のうえ、各１通を保有する。

●年●月●日

（甲）

（乙）

（※１）規定上は双務的な契約としているが、ここでは、主に自社が開示側となることを想定し、監査条項を含めている。

（※２）取引先との契約の場合、管轄地について双方が譲らないことも少なくなく、かかる場合には、本条項のように、いわゆる被告地主義に基づき、規定することが考えられる。

××有限公司　　出入登记表

＊来本公司参观、会晤、洽谈的各位，请在出入本公司时，填写下列表格。

＊出于对本公司信息的保密，希望您同意右侧保证书的内容，并在下表中的“同意上述保证书”一栏中做记号。

＊若您不同意右侧的保证书，我公司将拒绝您的出入，请谅解。

××有限公司

保证书

××有限公司

在贵公司参观、会晤、洽谈时，本人保证遵守下列事项。

第1条（保密）
本人将遵守以下事项。
① 未经贵公司负责人同意的，不在工厂内或办公场所拍照、录音、录像。
② 未经贵公司的事先书面同意，不将在贵公司工厂或办公场所内获得的信息对外转述或另作他用。
③ 不会将在贵公司工厂或办公室内获取的信息用于本次访问贵公司以外的目的。

第2条（损害赔偿）
本人同意，如违反上述规定事项，给贵公司带来损失的，本人将承担一切责任，并由本人所属公司和本人依据相关法律、法规的规定，对贵公司承担赔偿责任。

以上

NO	日期	公司名称	姓名	目的	进门时间	出门时间	同意上述保证书	拍摄许可	负责人签字
	2018/11/20	●●	●●	●●	10:00	15:00	✔	有/(无)	
1					:	:		有/无	
2					:	:		有/无	
3					:	:		有/无	
4					:	:		有/无	
5					:	:		有/无	
6					:	:		有/无	
7					:	:		有/无	
8					:	:		有/无	

＊粗线方框内：供来访者填写　　页码

5．来訪者受付表（中国語版）

＜参考和訳＞

××有限公司　　出入記録

＊当社に見学、面会、商談にお越しの方は、当社にお入りになる際、以下にご記入をお願い致します。

＊当社の情報の秘密保持のため、右の保証書の内容にご了承頂き、下表の「上記保証書に同意」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、当社への立ち入りをお断りする場合がございますことを、ご了承願います。

××有限公司

保証書

××有限公司

貴社における見学、面会、商談の際には、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、工場内又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、貴社の工場又はオフィス内で知得した情報を外部に伝達又は目的外使用しません。
③ 貴社工場またはオフィス内で知得した情報を、今回の貴社訪問の目的以外で利用しません。

第2条 （損害賠償）
上記規定に違反し、貴社が損害を被った場合、一切の責任を負うこと、及び、所属会社とともに、関連法律、法規の規定に基づき、貴社に対して賠償責任を負うことに同意します。

NO	日付	会社名称	氏名	目的	来社時刻	退出時刻	上記保証書への同意	撮影許可	サイン
	2018/11/20	●●	●●	●●	10:00	15:00	✔	有/(無)	
1					:	:		有/無	
2					:	:		有/無	
3					:	:		有/無	
4					:	:		有/無	
5					:	:		有/無	
6					:	:		有/無	
7					:	:		有/無	
8					:	:		有/無	

＊来訪者の方は、太枠内にご記入ください

No.

（※）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。

［著者］
上海擁智商務諮詢有限公司（IP FORWARD 法律特許事務所）
日本国弁護士　本橋　たえ子
（執筆協力）
上海擁智商務諮詢有限公司（IP FORWARD 法律特許事務所）
中国弁護士　周　婷

経済産業省委託事業

インドにおける営業秘密管理マニュアル

2024 年 3 月

独立行政法人　日本貿易振興機構

ニューデリー事務所

目次

はじめに

インドに進出し、又はインド企業と取引のある日本企業にとって、自社の技術及び営業秘密を守ることは極めて重要である。もし自社の技術及び営業秘密の保護がおろそかになれば、自社の技術及び営業秘密は簡単に社外に流出して、他社によりそれらが利用されることになり、当該日本企業の競争力は減退していくことにもなりかねない。従って、日本企業としては、とくに自社の技術及び営業秘密が重要な財産であることを肝に銘じるべきである。 ところが、近時、日本企業のそのような技術及び営業秘密が、様々な原因によって、中国、アジア等を初めとする海外において流出しているという問題が増えている。日本企業が自社の技術及び営業秘密を盗まれることは死活問題であるため、最近では、各日本企業において、営業秘密管理が新たな経営課題として認識されるようになってきている。 そこで、本稿では、インドにおける営業秘密管理に関する法制度及び具体的な紛争事例を紹介するとともに、日本企業のとるべき実務上の対策について考察することとしたい。

第１章 －インドの法制度－

1.　インドにおける営業秘密の定義：営業秘密の定義、営業秘密の認定要件等（WTO・TRIPS 協定及び日本法（例えば不正競争防止法）とインド法との違い）

(1)　インドにおける営業秘密の定義

インドにおいては、同国が世界貿易機関（WTO）に加盟し、「知的財産権の貿易関連の側面に関する協定（以下、「TRIPS 協定」という。）」を含むＷＴＯ設立協定に署名した後、営業秘密の概念が発展してきた。TRIPS 協定により、すべての加盟国には、同協定第 39 条に則り、営業秘密（Trade Secrets）や開示されていない情報（undisclosed information）[1]の保護が義務付けられている。

TRIPS 協定は、営業秘密の保護を規定し、ある情報が営業秘密に該当するかどうかについて以下の３つの要件を定めた初の多国間協定である。

(i)　当該情報は、秘密でなければならない。すなわち、一般的に入手不可能、又は、通常当該種類の情報を取り扱う者に知られていない

(ii)　秘密であることをもって商業的価値が生まれるものでなければならない

(iii)　その保有者は、当該秘密を保護するために合理的な措置を講じていなければならない

TRIPS 協定は、営業秘密とはどのようなものか、及び営業秘密の保有者が求め得る救済の種類について明らかにしている。一方で、同協定では営業秘密に関わる権利の形式・形態について規定されていないことから、加盟国には、特別の法令により保護すること、又はコモン・ロー（慣習法）制度を通じ、営業秘密を保護する裁量が認められている。

インドには、営業秘密の保護に関する特別法は存在していない。しかし、インドは WTO の加盟国であり、TRIPS 協定に従い、エクイティ（衡平法）及びコモン・ロー（慣習法・判例法）に基づき、営業秘密を保護している。営業秘密の保護に関する特別な法令が存在しないことから、営業秘密の保護は、裁判所の判断及び判例を根拠としている。

カルカッタ高等裁判所は、Fairfest Media Ltd 対 Lte Group Plc and Ors 訴訟判決

[1] TRIPS 協定では、「開示されていない情報（undisclosed information）」の語が用いられているが、本報告書では、協定条文を引用する場合を除き、営業秘密など適宜分かりやすい言葉を用いて説明を行うこととする。【MHM:原文になく出典不明】

（2015年）において、「この法律分野の本質は、その起源の如何にかかわらず、守秘の条件下で情報を入手した者が、当該機密情報を伝えた者に損害を与える活動のために、入手した情報を踏み台として利用することは認められないということである。」と判示している。インドの判例法は、営業秘密／機密情報、営業秘密が保護されるための根拠、又は救済の範囲を定義するなど、営業秘密保護の様々な側面への対応を試みてきた。インドの裁判所は、広く英国の判例法に依拠してきたが、現在では、増加する営業秘密保護に関する国内判例に依拠することが増えている。

営業秘密とは、事業にとって価値のある機密情報である。営業秘密／機密情報には、大きく分けて以下の２つのカテゴリーがある。

(i)　製品構造やレシピ、製品設計、製造工程、コンピュータコードなどの技術情報
(ii)　データベース、顧客リスト、消費者の嗜好、価格情報、販売及び事業計画などの事業や財務情報

営業秘密とは、競合他社に対する市場における優位性を事業や企業にもたらすすべての情報を指し、商業的価値のあるコンセプト、ノウハウ、技術が含まれる。営業秘密は、本質的に、組織や企業にとって極めて重要なものであり、法的、倫理的、又はその他の理由で公になることなく秘密に保たれてきたものである。
営業秘密の例としては、ビジネスプロセス、顧客リスト、製品構造、製造工程、ソフトウェアコード、技術データなどがある。

インド政府の知的財産権振興管理支局（CIPAM:The Cell for IPR Promotion and Management）が公表した営業秘密保護のためのガイドブック[2]別紙Aにあるように、「営業秘密」とは、企業にとって商業的価値があり、それを秘密に保持することにより優位性が得られる情報を指す。ここで「秘密」とは、当該情報を窃取又は漏洩されないようしかるべき措置を意識的に講じることにより秘密が保持された情報をいう。機密情報は、社外に知られてはならず、他者に容易に知られるようなものであってはならない。営業秘密には、製品構造やレシピ、製造工程、サプライヤーや顧客リスト、製造ノウハウ、顧客向け仕様書、消費者の嗜好、技術設計、青写真、価格情報、販売及び事業計画などがある。

[2]「営業秘密保護のためのガイドブック」
http://cipam.gov.in/wp-content/uploads/2019/10/Tradesecret-Toolkit-1.pdf

インドには営業秘密の保護を規定している固有の成文法はないが、裁判所では、判決に当たりBlack's Law Dictionary（第８版）記載の定義が広く参照されている。The Black's Law Dictionary（第８版）では、営業秘密を以下のように定義している。

「競合他社に対して優位性を維持するために機密として保持されている製品構造、工程、デバイス、その他の事業関連情報であって、製法、パターン、編集物、プログラム、デバイス、手法、技法、工程を含む情報であり、

(i) それが一般的に知られていないこと又はその開示又は使用から経済的価値を得ることができる他者が容易に確認できないことから、実際の又は潜在的な独立した経済的価値を生じさせるものであり、かつ

(ii) 当該状況下において、その秘密性を維持するための合理的措置を講じる対象となるもの。」

この考え方については、Tata Motors 対西ベンガル州[3]訴訟判決においても触れられており、同判決では、「より大きな公益のため当該情報を開示すべきだと監督当局が認めた場合を除き、いかなる市民対しても、商業上の機密、営業秘密、知的財産等の開示されることにより第三者の競争上の地位を損なうこととなる情報を開示する義務は存在しない。」と判示している。

1995 年 10 月 20 日のデリー高等裁判所による Burlington Home Shopping Pvt 対 Rajnish Chibber 訴訟判決は、営業秘密とは、パブリックドメインとして入手することができず、開示によりその保有者に多大な損害を与える、商業的価値を有したあらゆる情報だとしている。

2010 年のボンベイ高等裁判所による Bombay Dyeing 及び Manufacturing Co. Ltd. 対 Mehar Karan Singh[4]訴訟判決は、情報を営業秘密と分類するために必要な要素として以下を挙げた。

(i) 当該情報が機密として保持されている度合
(ii) 当該情報が企業内部の人間に知られている度合
(iii) 当該営業秘密の機密性を守るために保有者が講じた対策
(iv) 当該営業秘密が開示された場合の当該企業の製品やサービス価格への影響

[3] Tata Motors Limited vs West Bengal Industrial ... AP NO.285 OF 2018 on 22 November 2018 IN THE HIGH COURT AT CALCUTTA By Hon'ble JUSTICE ARINDAM SINHA (https://indiankanoon.org/doc/109815302/)

[4] Bombay Dyeing and Manufacturing Co Ltd v Mehar Karan Singh (2010 (112) BomLR 375) on 24 August 2010 in High Court of Bombay by Hon'ble Justice: R. S. Dalvi[5] ANNEX 1C

度

(v) 当該情報の入手、開発並びに保護に要する労力又は費用

(vi) 当該情報の複製、取得又は盗用に要するであろう時間及び費用

(1) 営業秘密の認定要件等

インドには、営業秘密に関する成文法が存在しないが、インドは WTO 加盟国であるため、TRIPS 協定第 39 条第 2 項に基づき、情報が営業秘密として認められるための要件として以下を認めている[5]。

a) 当該情報が一体として又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又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

2015 年３月 25 日の Beyond Dreams Entertainment Pvt.対 Zee Entertainment Enterprises 訴訟判決（NOTICE OF MOTION (L) NO. 785 OF 2015 IN SUIT (L) NO. 251 OF 2015 on 25 March, 2015 IN）[6]において、ボンベイ高等裁判所は、秘密保護の申立を満たすために重要な３要素について、以下の通りとしている。

(i) 第一に、当該情報そのものが秘密性を有することが示されなければならない。

(ii) 第二に、被告に秘密保持義務を課した上で、当該情報が被告に開示又は伝達されたことが示されなければならない。言い換えれば、両当事者間には秘密保持の関係が存在しなければならない。

(iii) 第三に、共有された情報が、被告によって権限のないまま、すなわち、原告の許諾がないまま実際に使用され、又は使用されるおそれがあることが示されなければならない。

---

[5] ANNEX 1C

AGREEMENT ON TRADE-RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS (TRIPS Agreement)

SECTION 7: PROTECTION OF UNDISCLOSED INFORMATION (Article 39)

[6] https://indiankanoon.org/doc/162638144/

これら三つの基本要素のそれぞれは、同時に留意する必要がある独自の特殊性と副要素を含んでいる。

（2） 営業秘密とは見なされない情報[7]

これに対して、以下の情報は、営業秘密とは見なされ得ない。

（i） 製品発売後に当該製品を確認/研究することにより、競合他社が容易に見つけることのできる情報。これは、製品発売前は当該製品情報は秘密とされていても、発売後は秘密とはならないためである。

（ii） 個人が調査を通じて独自に開発した情報。これは、個人は自らが保有する秘密情報の他者による利用を止めさせることができるものの、他者が独自の調査により同一の情報を開発した場合、当該個人はこれらの他者による利用を止めることができないためである。

（iii） 既にパブリックドメインとして入手可能である情報。例えば、インターネット上で公開されているものは、もはや営業秘密とはなり得ない。

（iv） 企業の従業員が自ら獲得したスキルや知識は、当該企業がこれを営業秘密とすることはできない。これは、従業員は、退社する際に機密情報を持ち出すことはできないものの、当該企業で学んだ一般的なスキルや知識を活用することは可能であるためである。このため、営業担当者は顧客リストを持ち出すことはできず、生産管理者は製品レシピを持ち出すことはできない。しかし、競合他社に転職した後に、前職において学んだスキルを活用することはできる。

（3） インド法と WTO・TRIPS 協定との比較

インドには営業秘密の保護に関する特定の、又は独自の法律は存在しない。しかし、インドの裁判所は、契約法、著作権法、衡平法[8]の原則など多くの法令・法規範の下で、また、ときにコモン・ローにおける守秘義務違反訴訟において、営業秘密の保護を認めてきた。したがって、本マニュアルにおける営業秘密の保護に関する説明は、インドにおける営業秘密の保護を規定したさまざまな法律・法規範についてのものである。

（4） インドには営業秘密法は存在しないが、営業秘密保護について

[7] http://cipam.gov.in/wp-content/uploads/2019/10/Tradesecret-Toolkit-1.pdf

[8] 衡平法(equity)：英米法を採用する国々において、コモン・ローによって解決できない事柄に適用される法律等。【MHM:原文にない、出典不明。】

WTO・TRIPS 協定に準じている9

インドはパリ条約の締約国であるため、TRIPS 協定第１条第２項が、同協定が対象とする知的財産権に、開示されていない情報の保護が含まれると規定していることに言及すべきであろう。インドは、TRIPS 協定の署名国であり、加盟国として、情報の不正な開示を防止することにより営業秘密を保護するため法律を形成する柔軟性を有している。インドには営業秘密に関する特定の法律や法規はないが、インドの裁判所や法廷は、契約法、著作権法、衡平法、コモン・ローにおける守秘義務違反訴訟（基本的には情報の秘密保持義務違反）などの他の法律に基づいて営業秘密の保護を支持してきた。上記に加え、2000 年の情報技術法には、電子記録の形式の機密情報を保護する法的手段も定められている[10]。

営業秘密とは、1995 年 10 月 20 日に Burlington Home Shopping Pvt.対 Rajnish Chibber 訴訟判決においてデリー高等裁判所が示したように、パブリックドメインではなく、商業的価値を有し、かつ、開示された場合、保有者に重大な損害をもたらす情報である。同時期の 1995 年に成立した TRIPS 協定は、営業秘密を「秘密として保持され、商業的価値を有し、かつ、情報の保有者が秘密保持のために合理的な措置を講じる情報」と定義している。したがって、インドの裁判所は、WTO・TRIPS 協定と同じ定義・要件を用いている。

世界知的所有権機関（WIPO）は、営業秘密に関する国際的な規定をコントロールしている。WIPO は、どのような情報が営業秘密として認定されるかについての基準が国により異なることを認めているが、知的所有権の貿易関連の側面に関する協定（TRIPS 協定）第 39 条にはいくつかの一般的な基準・要件が規定されている。

TRIPS 協定第 39 条は、開示されていない情報、すなわち営業秘密の定義及びその侵害について言及している。同条は、加盟国は、自然人又は法人が、自己の管理する情報が公正な商慣習に反する方法により、自己の承諾を得ないで他の者により開示、取得又は使用されることを防止する「可能性」を確保しなければならないと規定している。ここで触れられた「可能性」とは、営業秘密は加盟国の何らかの国内法制度の枠組み内で保護されるべきものであり、必ずしも当該加盟国の知的財産に関する法的枠組みにおいて保護される必要があるわけではないことを意味しているものと考えられる。このため、以上で見たように、インドは、独自の制度に従い、契約法に基づく契

[9] https://www.wto.org/english/tratop_e/trips_e/tripfq_e.htm#Who'sSigned

https://www.wto.org/english/docs_e/legal_e/27-trips.pdf 3

[10] https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/short-introduction-trade-secrets-india-2021-11-05_en

約の保護のように、コモン・ロー[11]の下で、情報を保護している。

TRIPS 協定第 39 条第２項では、ある情報を営業秘密と認めるための要件として、以下の三つを規定し、これに合致する自然人又は法人の管理下にある情報の保護を WTO 加盟国に義務付けている。

(i)　当該情報は、一体として又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一般的に知られておらず又は容易に知ることができない
(ii)　当該情報は、秘密であることにより商業的価値がある
(iii)　当該情報は、それ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

したがって、WTO・TRIPS 協定の要件を遵守するインドは、情報を営業秘密であると判断するか否かについて、WTO・TRIPS 協定と近似した定義と要件を用いている。

(5)　インド法と日本法との比較

日本において「営業秘密」とは、不正競争防止法により、以下の３つの要件を満たす技術上又は営業上の情報をいう（第 2 条第 6 項）。

(i)　秘密として管理されている（秘密管理性）
(ii)　[生産方法、販売方法その他の事業活動に]有用な技術上又は営業上の情報である（有用性）
(iii)　公然と知られていない（非公知性 or[非パブリック・ドメイン]）

日本は、パリ条約に従い 1934 年に制定され、営業秘密を保護するため 1990 年に改正された不正競争防止法を有する。不正競争防止は、上記の改正に加え、1993 年に全面改正された。この法律の目的は、事業者間の公正な競争を確保し、事業者の健全な育成とそれに関連する国際協定の正確な履行を図り、もって国民経済の健全な発展に貢献するため、不正競争の防止、不正競争による損害の賠償といった措置を定めることである。

比較をすると、インドでは、日本と類似した営業秘密の定義を有している。それは一般的に知られておらず又は容易に知ることができない、秘密であることにより商業的

[11] コモン・ロー（common law）：イギリスにおいて発展した先例（判例、伝統、慣習等）に重きを置く法体系。【MHM：原文にない。出典不明。】

価値がある、及び秘密保持のための合理的措置を講じられた価値ある商業的な情報というものである。

2.　インドにおける営業秘密侵害の定義

侵害等と見なされる行為の説明（WTO・TRIPS 協定及び不正競争防止法等の日本法と比較したインド法の説明）

許諾を得ない商業的価値のあるあらゆる情報開示、違法な利用は、「営業秘密の侵害」に当たる。営業秘密の侵害は「不正利用」とも呼ばれる。

営業秘密の不正利用を定義した法律は存在しないが、不正な手段（契約違反又は不法行為などに起因する民事上の行為、もしくは犯罪行為）による営業秘密の開示は、営業秘密の不正利用に当たる。

一方、インドの裁判所は、営業秘密が不適切に使用された際に救済を提供するために、(制定法の）代わりにコモン・ロー及び衡平法の原則に依拠してきた。秘密情報を開示された者は、機密保持の条件の下に同者に与えられた情報を秘密に保持するよう契約上要求され得る。この場合、情報の一部が公知（public knowlege）であったとしても、秘密保持契約がある限り、当該契約に反して用いることはできない。秘密保持契約に違反した者は、損害賠償を求め訴えられる可能性がある。

1989 年のインドに関する GATT のディスカッションペーパー[12]によれば、営業秘密を知的財産権と見なすことはできない。この 1989 年の GATT のディスカッションペーパーは、貿易関連知的財産権の利用可能性、範囲及び利用に関する基準及び原則につい

[12] https://www.wto.org/gatt_docs/english/sulpdf/92070115.pdf

ての交渉グループのメンバーに回付された「貿易関連の知的財産権の利用可能性、範囲及び利用に関する適切な基準及び原則の規定」に関するインドの見解を示している。当該文書は、知的財産権の基本的要素はその開示、公表、登録である一方、営業秘密は秘密保持を前提としたものだとしている。当該文書は、知的財産法ではなく、適切な民事法と契約上の責任が、秘密性及び守秘義務の遵守と執行を規制すべきであると続けている。

しかし、日本をはじめとする国々には、営業秘密の侵害を規律する特別な法律が存在する。日本における営業秘密の保護は不正競争防止法によって規定されている。

この法律に基づく営業秘密とは、次のような技術情報又は営業上の情報を意味する。

i. 生産方法や営業方法などの商業活動に有用であり、秘密にされるもの

ii. 秘密にされておりかつ有用性がある

iii. 公には知られていない、パブリック・ドメインでない

中国[13]、韓国[14]、ドイツ[15]、ポーランドでは、営業秘密は不正競争関連の一般法の下で保護されている。

米国[16]では、営業秘密保護制度は、連邦法及び州法の両者の下で成文化されている。

インドにおいて営業秘密の不正利用を証明するには、営業秘密の保有者又はその権利者は、2015 年 3 月 25 日の *Beyond Dreams Entertainment Pvt.対 Zee Entertainment Enterprises 訴訟判決（NOTICE OF MOTION (L) NO. 785 OF 2015 IN SUIT (L) NO. 251*

[13] https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/outreach_r3_korea.pdf

[14] https://www.meti.go.jp/policy/economy/chizai/chiteki/besshireiwa.pdf

[15] https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/outreach_r3_europeanduniteds tates.pdf

[16] https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/outreach_r3_europeanduni tedstates.pdf

OF 2015）においてボンベイ高等裁判所が示した以下のような要件を証明しなければならない。同裁判所が判示した要件は以下の通りである。

(i) 当該情報は秘密であり、かつ、一般に知られておらず、又は当該情報に類する情報を取り扱う者が容易にアクセスすることができないものであったこと

(ii) 個人又は当該情報の保有者が、その秘密性を確保・維持するために合理的な措置を講じ、当該情報が秘密保持義務を課す状況において伝達されたこと

(iii) 当該情報を伝達した当事者に損害が生じるような不正に使用があったか、又は当該情報が不正に使用されるおそれが生じたこと

契約違反に適用される法的責任についてのコモン・ローの原則は、営業秘密の不正利用の事案にも適用される。一般に、何らかの作為又は不作為を通じて、営業秘密の不正利用に手を貸した者は、かかる不正利用に対して直接かつ共同で法的責任を負わされる可能性がある。また、当該事案の事実及び状況により、代理人及び代位責任の原則が適用される場合もある。さらに、間接侵害の考え方は、インドにおける著作権に関する法律である 1957 年著作権法（ACT NO.14, 1957 [1957 年 6 月 4 日]）でも受け入れられており、従って、対象物が著作権法に基づいて保護されている場合、これらの原則が適用される。間接侵害は、特許、著作権、又は商標の直接侵害に対する二次的責任の一形態である。これは、実際に侵害行為を行っていない者も、侵害の責任を問われる可能性がある法的手段である。たとえば、ソフトウェアデータベースの場合、著作権法で保護されている編集物が元従業員によってコピーされ、現在の雇用主のビジネスを促進するために使用されたような場合である。現在の雇用主は、そのようなソフトウェアが別の会社に帰属することを知りながら、これを使用すること及び自分のコンピュータ又はサーバーにアップロードすること

を許可していた場合、間接責任又は間接侵害の責任を負うことになる。

間接侵害の概念は、著作権侵害に直接関与していないかもしれない海賊版ソフトウェアや映画などを配信するオンラインウェブサイトやポータルに対しても適用される。当該ソフトウェアが侵害されていることを知り、かつこれらを配信し又はビジネスを促進するために利用することにより金銭的利益を得ていたという事実は、これらの者に、直接侵害ではないにしても、間接侵害の責任を負わせることになる。

刑法犯となる背任又は窃盗の場合、そのような犯罪を幇助又は教唆する者は、インドにおける正式な刑法典である 1860 年インド刑法（ACT NO.45, 1860［1860 年 10 月 6 日］。IPC（The Indian Penal Code)。以下「インド刑法」という。）に基づいて処罰される責めを負う。これは、インドにおける刑法のあらゆる実体的側面を網羅することを意図した包括的な法律である。

通信及び秘密情報の保管における情報技術（IT）の活用が増大したことで、電磁的ルートを通じた情報の窃盗及び悪用に対する民事上及び刑事上の救済を提供する必要性が生じている。

2000 年 IT 法において、「データ」とは、情報、知識、事実、コンセプト又は指示を表すものであり、一定の形式を用いて作成されつつある又は既に作成されており、処理されることを想定され、コンピュータシステム又はコンピュータネットワークで処理されつつあるもの又は既に処理されたもの、及び、何らかの形式（コンピュータ印刷物、磁気又は光学記憶媒体、パンチカード、パンチテープを含む）又はコンピュータのメモリ内に格納されることを想定されているものを意味する。IT 法は、電子商取引も対象とし、以下の事項に対する罰則を規定している。

(i)　コンピュータフレームワークへの不正アクセス

（ii） コンピュータフレームワークのプログラミングの破壊

（iii）データの不正なダウンロード又は複製

（iv） コンピュータ・ソースコードの改ざん

（v） コンピュータフレームワークへの不正ハッキング

（vi） 保護されたフレームワーク内で保持された情報へのアクセスとその悪用

（vii）IT 法に基づく権限に同意した者による機密保持及びデータ保護違反

インド刑法は「窃盗」を定義し、すべての有形資産を含む動産の窃盗に対する罰則を定めている。この規定により、無形資産であるデータはインド刑法の対象外であることが明確化されている。ただし、フロッピーディスク、CD、ペンドライブ、ハードドライブ等の媒体に情報が保管されていた場合、被告人に刑事罰を科すため、インド刑法における窃盗関連条項を適用することができる。

IT 法第 66 条は、データ窃盗からの保護に関するものであり、第 72A 条は正当な契約に違反してなされた情報開示に対する罰則を規定している。これらの条項は、いずれも３年以下の禁錮又は 50 万ルピー以下の罰金、又はその両方を含む刑罰を規定している。IT 法第 43 条（b）は、不正なダウンロード、複製、情報・データ・データベースの抽出に対し、数千万ルピーに上る場合すらある民事上の多額の損害賠償金を課すことにより、保護を提供している。第 43 条（c）は、コンピュータウイルスその他のマルウェアが不正に侵入した場合の補償について規定している。以上で見たように、データ窃盗は、事案の事実に応じて、1860 年インド刑法、2000 年 IT 法及び 1957 年著作権法の対象とすることが可能である。

3. インドにおける営業秘密侵害種別の例

具体的な侵害の種別、新たな侵害の種別（在宅勤務等の新たな働き方における侵害等）等

(1) インドにおける営業秘密侵害の例と侵害に関する新規、又は具体的種別

インドでは、営業秘密関連係争の大半が、従業員、ベンダー、又は競合他社による機密事業関連情報について、その保有者が意図しない漏洩をめぐるものである。営業秘密侵害事件のほとんどはクライアント又は顧客情報、技術情報、ベンダー情報の不正利用/窃取に関するものである。以下に、その例をいくつか挙げる。これらの例については、判例に基づき説明する。

・顧客の詳細、顧客の連絡先、ベンダーの詳細、流通網に関する情報、広告戦略
・食品レシピ
・特定のソフトウェア又はソフトウェアコードのためのコンピュータプログラミング
・事業計画
・データベース
・意匠
・美容製品の製法
・技術的プロセス
・価格情報・財務情報等

例えば、自動車メーカー又はエンジニアリング会社の設計部門に勤務するある従業員は、勤務先の秘密保持された設計情報にアクセス可能である。

この従業員が、会社のサーバーから設計情報を盗み出し、勤務先の競合相手に金銭的報酬の見返りとしてそれを売り渡す、といったケースが考えられる。

2022年6月3日のデリー高等裁判所による Anil Gupta 対 Kunal Dasgupta 訴訟判決（2002 IVAD Delhi 390, AIR 2002 Delhi 379, 97 (2002) DLT 257）では、原告は、テレビの恋愛リアリティショーである「Swayamvar」のコンセプト発案者であった。原告は、被告にこれに関するコンセプトノートを提供した。その後、原告は、被告らが自らのアイデアに基づき注目度の高いリアリティショーをスタートさせようとしていることを新聞記事で知った。原告は差止請求を申し立てた。

裁判所によれば、原告のアイデアは、パブリックドメインである可能性のある題材に創作した結果として創造され、発展されたものである。しかし、原告がこのコンセプトを応用するために自らの頭脳を使い、唯一無二の結果に至ったことは、そのアイ

デアに専有権を与えるとして、裁判官は差止命令を出した。裁判所の決定は、アイデアそれ自体には著作権はないが、相応の詳細を含むコンセプトにまでそれを昇華するなら、登録が可能となり、著作権法に基づいて保護されることになるという事実に立脚したものである。コンセプトノート及びその中の機密情報の無断使用は権利の侵害となる。

インドにおいて、裁判所はこの事件を通じ、コンセプトノートが著作権法の下で著作権保護の対象となり得ること、及びオリジナルのアイデア、コンセプト又はテーマを生み出した人がその労働に対して確実に対価を得られるようにしなければならないことを初めて認めた。

続いて、以下の判例では、営業秘密が裁判所により認定、あるいは認定されなかったさまざまな状況を概説する。

デリー高等裁判所による 1987 年 7 月 6 日の Richard Brady 対 Chemical Process Equipments P Ltd（AIR 1987 Delhi 372）訴訟判決では、飼料用機械の図面及び技術的知識が不正利用された事案が扱われている。本件は、契約が存在しない場合の秘密保持義務の原則に関する初の訴訟の一つであった。デリー高等裁判所は、「本件については秘密保持契約の有無に関わらず、秘密情報を受領した者はその情報を不当に利用してはならないという、広範な衡平法の原則に依拠している」との判断を示した。また、同裁判所は、営業秘密侵害であるかどうかについて、被告らに対し、「厳格な秘密保持に関する条件が明示された下で委ねられたにもかかわらず、市場参入のきっかけとして利用することで原告らに損害を与えた」として、原告の機械に関するノウハウ、仕様書、図面その他の技術情報をみだりに利用することを禁じた。本件においては、図面、技術知識、ノウハウ、仕様書、図面等の技術情報が営業秘密として認定された。

デリー高等裁判所による 2006 年 5 月 8 日の Diljee Titus Advocate 対 Alfred Adebare 訴訟判決（130 （2006） DLT 330）は、顧客データの不正持ち出しについて扱われたものである。本件において、Mr. Diljeet Titus、Mr. Alfred Adebare その他のアソシエートは、ある法律事務所の同僚であった。その後、Mr. Adebare らはその法律事務所からの退所を決めた。退所手続き中に、被告らは、Mr. Titus と働いていた際に作成したクライアントの連絡先をすべて持ち去った。彼らの行動により権利を侵害された Mr. Titus は、彼らを提訴した。

裁判所は、Mr. Adebare らは自由に職業を営み、身に付けたスキルや記憶した情報を利用することができるとしつつ、Mr. Titus が専有的に権利を有する顧客名簿等の使用についてのみそれを禁じるとの判断を示した。

契約書は存在しないものの、守秘義務の下で入手可能であった Mr. Titus の資料を利用する権利は Mr. Adebare らにはないとされた。裁判所によれば、過去に原告と共に働いていた Mr. Adebare らは、契約書、デュー・ディリジェンス・レポート、顧客リストなど、Mr. Titus と同僚であった間に知り得たあるいは開発された資料、又はそれ自体が機密であり、したがって営業秘密と認定される文書や情報である資料は、それがどのようなものであれ使用することはできない。本件において、顧客の連絡先や顧客リスト、契約、デュー・ディリジェンス・レポートが、営業秘密であると認定された。

マドラス高等裁判所による 1954 年 12 月 1 日の Govindan 対 Gopalakrishna 訴訟判決（AIR 1955 Mad 391）では、裁判所は、顧客データの漏洩を認定した。本件における営業秘密の対象は、顧客データについての編集物であった。編集物における独自性（オリジナリティ）は量的には僅かであるが、この僅かな独自性は法により保護されるとの判断が示された。従って、いかなる当事者も、たとえそれが編集物内のものであっても、他方の当事者の情報収集、スキル又は労働の成果を窃取し、又は利用することはできない。 本件において、顧客データの編集物は、営業秘密として認定された。

デリー高等裁判所による 1995 年 10 月 20 日の Burlington Home Shopping Pvt. 対 Rajnish Chibber 訴訟判決（第 1 部にも記載）は、クライアントや顧客とその住所に関する編集物からなるコンピュータデータベースに関するものであった。同裁判所は、時間、費用、労力、スキルを費やして作成された住所関連編集物は（情報源は広く入手可能なものである可能性はあるものの）著作者が著作権を有する文学作品に相当するとの判断を示した。被告のデータベースが事実上原告のデータベースの複製であると判断した裁判所は、仮差止命令を下した。本件において、クライアントや顧客及びその住所についての編集物であるデータベースは営業秘密であると認定された。この訴訟の争点は、連絡先のデータベースが「オリジナルの文学作品」を構成するかどうか、したがって著作権を発生させるかどうかであった。裁判所は、「情報の入手源が共通であるとしても、何人かが時間、お金、労力、技術を費やして作成したアドレスの編集物は、その作者が著作権を有する『文学作品』に相当する」と判示した。このほか、データベースとしての顧客リストも秘密情報や営業秘密に関する法律で保護されている。したがって、この訴訟では裁判所によって二重の保護が認められた。

インド最高裁判所による Superintendence Co. of India Pvt. Ltd. 訴訟判決（1980 AIR 1717, 1980 SCR (3)1278）において、被告である従業員は原告の品質評価のための製品検査技術を窃取したとされた。原告は、品質試験と品質管理のための独自の技術を開発し、当該技術及び同社顧客は営業秘密であると主張した。本件において、Superintendence Company of India 社は、製品品質評価のための製品検査業務を営ん

でおり、品質試験及び品質管理技術を開発し、これを営業秘密として保護していた。Mr. Krishnan は同社の管理職として雇用されていた。

同社を退職後、Mr. KrishnanはSuperintendence Company と競合他社を立ち上げた。Mr. Krishnan は、原告企業の競合他社と提携し、同社の顧客層である顧客/企業の引き抜きを図った。Mr. Krishnan はまた、同社雇用期間中に知り得た Superintendence Company の秘密技術を利用した。

Mr. Krishnan により製品検査技術を窃取された Superintendence Company は、雇用期間中の同氏との契約内容と同等の活動を被告に禁じる終局差止命令を求め、提訴した。また、Superintendence Company は、同氏による新規事業又は雇用の継続を禁ずる仮差止命令を求めた。本件において同最高裁は、Mr. Krishnan に対しては、同社の営業秘密の開示についてのみ禁止することができ、同社と競合関係にある事業を営む、あるいはそのような事業で雇用されることを禁ずることはできないとの判断を示した。以上のとおり、品質評価のための製品検査技術としての営業秘密は、本件において裁判所により認定された。

このように、ここで紹介したインドの裁判所による判決からは、営業秘密の確実な保護のために、その保有者は契約書又は契約書中の秘密保持条項を拠り所にできるということが明らかである。契約書又はその中の秘密保持条項は、通常、機密情報を秘密として保持し、雇用期間中及び雇用期間終了後に漏洩しないことを従業員に要求するものである。従業員が契約に違反して退職した場合、一定期間同様の活動に従事しないことを義務付ける競業避止条項の遵守を当該従業員が求められる場合もある。ただし、機密情報又は営業秘密の漏洩に関する雇用主と従業員との間の係争に対して、裁判所の判断は、生活を営むための権利を考慮して従業員寄りのものとなる可能性がある。

4. インドにおける営業秘密保護制度

インド等における営業秘密に関する法律、制度その他の法的措置（(A) 判例法及び/又は制定法、(B) 民法、刑法、労働法、営業秘密保護法、その他の法律、(C) 民事救済及び/又は刑事制裁及び/又は行政上・多国間の措置等）

5. 営業秘密侵害に対する法的手続

法的手続に関する説明。具体的かつ実践的な手続は、第２部～第３部に記載。

インドは TRIPS 協定の締約国であり、加盟国として、情報の不正な開示を防止し、営業秘密を保護するための立法の自由を有している。インドには営業秘密に関する特別な法律は存在しないが、インドの裁判所や調停機関（tribunals）は、契約法、著作権法、衡平法の原則、機密情報の保護に対する法的措置を定めた 2000 年 IT 法などの多くの法律の下で、また、ときにコモン・ローにおける守秘義務違反（事実上、契約上の義務に対する違反に相当する）訴訟を通じて、営業秘密の保護を図っている。事業者が保有する機密データは、スタッフ、方針、手順、及び技術管理に関する包括的なセキュリティ戦略を実施することによって保護することができる。これにより、意図しない漏洩リスクの低減につながる可能性がある。

裁判所において、情報が「営業秘密」であると認められるためには、当該情報が「機密」として保持されるのと同時に、その情報の秘密性、秘密として保持されていることに基づく商業的価値、秘密保持のための合理的措置が採られているという３要件が全て満たされていることが重要となる。

〇一般論として、営業秘密と認定されるために当該情報が満たすべき要件は以下の通り

(i) 秘密であることにより商業的価値があり
(ii) 限られた集団に属す者のみが知っており
(iii) 取引相手や従業員に対する秘密保持契約締結等、正当な保有者が講じる当該情報を秘密に保持するための合理的な措置の対象である

NDA（秘密保持契約）は、重要情報である可能性のある情報が漏洩しないように、また、共有される情報が秘密であることを契約当事者又は契約先企業に認識させることを企図して締結されるものである。機密保持の条件の下に情報を開示された者に対しては、当該情報をいかなるものも開示してはならないという契約上の義務を負わせることができる。秘密保持契約に違反した者に対しては、損害賠償を求め、訴えを起こすことができる。企業は、従業員が当該企業に雇用されている間、又は従業員が当該

企業を退社してからも、当該企業に関連した機密情報及び秘密情報を当該従業員が開示することを防止する秘密保持契約を雇用契約に含めることができる。この契約により、当該企業は、従業員による機密情報の意図しない漏洩などを防止することができる。

(1)　救済策

管理・保有する情報の伝達及び保管における情報技術の活用が増大したことで、電磁的ルートを通じた情報窃盗及びその悪用に対する民事上及び刑事上の救済を提供する必要性が生じている。営業秘密の侵害は、法の執行の観点からは、民事上の措置、刑事上の措置のいずれにおいても対応が可能である。営業秘密の保有者は、侵害・違法行為を行った者が秘密情報を開示することを防止するため、差止命令及び損害賠償の請求を、裁判所に申立てることができる。もし営業秘密の保有者が、著作権法上及び IT 法上の侵害を立証できた場合、裁判所は、インド刑法、著作権法及び IT 法に基づき罰金又は禁錮刑を科することができる。民事訴訟による場合は、損害賠償及び差止命令による救済の可能性がある。

(2)　営業秘密の保有者が求めることのできる民事上の救済

Fairfest 訴訟において、裁判所は、営業秘密の保有者が求め得る救済措置としては、営業秘密の開示を防止するための差止命令の取得、すべての機密情報の返還、及び営業秘密の開示により被った損失に対する補償などがあるとした。これらの救済手段はすべて利用可能である一方、インドの裁判所は、営業秘密窃取への対応として差止命令という手段を広く用いてきた。その理由は、差止めが営業秘密の保有者に対し金銭的に見積もることのできない「回復不可能な損失」を生じさせる可能性のある侵害行為に対する唯一の実行可能な救済手段であるというものである。効果的な救済として、損害賠償に対して差止命令に優位性があることは、法律文献において広く認識されている。以下がその例である。Bombay Dyeing and Manufacturing Company 対 Mehar Karan Singh 訴訟（2008 年）において、ボンベイ高等裁判所は、原告の関連資産に関する機密情報の開示に対して差止命令を出し、これとは別の訴訟を通じて救済を求めることもまた認めた。

一般的に、差止命令が出された営業秘密の窃取事案の多くにおいては、被害を受けた当事者に、差止命令以外の救済が例外なく認められる。さらに、2000 年 IT 法は、法定損害賠償額を具体的に定めており、サイバー犯罪に対する救済として、通常、損害賠償その他の刑罰が科されることとなる。

刑事上の制裁は、IT 法第 72 条（２年以下の禁錮又は 10 万ルピー以下の罰金、又はその両方）及び 2012 年（改正）著作権法第 65A 条（２年以下の禁錮及び罰金）に基づ

き請求することができる。

また、電磁的記録に限定されるが、2000 年 IT 法第 72 条は、電磁的記録に対する一定の保護を提供している。

なお、インドにおいては、営業秘密は、(判例の積み重ねによる) コモン・ローの原則とインドの契約法の下で保護が図られており、さらに営業秘密に関する特別法が存在しないため、営業秘密の不正利用に対する行政上の措置は存在しない。

○　営業秘密の保有者は、任意に選択可能な以下の法的選択肢を有する。

(i)　ライセンシー、従業員、ベンダーその他の者が営業秘密を開示することを禁ずる差止命令
(ii)　すべての機密情報及び専有情報の返還
(iii)　営業秘密漏洩の結果生じた損失に対する補償

(3)　　契約法における営業秘密の保護

契約法の下では、契約や合意により第三者への情報開示を制限される場合がある。秘密保持契約 (NDA) は、当事者間で情報を共有する際に締結される。このような秘密保持契約、制限的条項又は合意は、契約法に基づき履行強制が可能となる。

(i)　上述のとおり、インドには営業秘密に関する特別法は存在しないが、インドの裁判所は、契約法、著作権法、衡平法の原則など様々な法令の下で、また、ときにコモン・ローにおける守秘義務違反 (事実上、契約上の義務違反となる) 訴訟において、営業秘密の保護を認めてきた。
(ii)　インドは、TRIPS 協定の締約国として、開示されていない情報 (営業秘密) を保護する義務を負っており、当該情報の保護のために、多くの場合、コモン・ローの原則を適用している。
(iii)　「営業秘密」を正式に認定する、又は定義する統一された法律が存在しないため、インドにおける機密情報の保護は、異なる種類の機密情報を認定し保護するインド契約法第 27 条及び情報技術法第 72 条の下での様々な規定に基づき行われる。

(4)　　契約が存在しない場合の機密情報の漏洩

Richard Brady 対 Chemical Process Equipments P Ltd 訴訟判決 (AIR 1987 Delhi 372) では、裁判所は、衡平法上の救済を与えるとの判断を下した。

○　事実

原告は、飼料市場に参入するために飼料生産ユニット（FPU）を開発した。原告は、上記の機械用感熱パネルの調達検討のための見積もりを依頼した。被告は、見積もりを作成するため、FPU装置に関するすべての図面及び技術知識を受領した。当該情報は、秘密保持契約に基づき提供され、契約が有効である間は、他のいかなる者もこれを入手・利用することはできないことが合意された。言い換えると、ここでのアクセスとは「機械を作るための情報が第三者に共有されないこと」を意味する。この場合のNDAの目的は、機械を製造するための見積もりを求め、当事者の能力を評価することであった。しかし、最終的な合意が署名されなかったため、供給の取引は実施され得なかった。原告は見積書を入手したが、最終契約（供給契約）には署名しなかった。

その後、原告の FPU 装置の操作方法を理解するために、被告が原告の FPU 装置を持って多くの地域を訪問していたこと、また、原告のものと同一の機械を製造していたことが判明した。

○　判決

本件において、裁判所は、当該機械に関する契約が存在しない中、差止命令を出した。この事件では秘密保持契約が結ばれていたようである。しかし、本件での NDA の目的は、機械を製造するための見積もりを求め、当事者の能力を評価することであった。同裁判所によれば、明示的な秘密保持条項がない場合であっても、関連する事実及び状況から秘密性を推し量ることは可能である。このような場合、被告は黙示の秘密保持義務に違反したとして責任を負うこととなる。

(5)　　機密保持、秘密保持契約違反

Diljeet Titus Advocate 対 Alfred A Adebare 訴訟判決（130（2006） DLT 330）において、裁判所は、被告が秘密保持契約に違反しているとの判断を示した。被告らによる秘密保持契約違反を受けて、裁判所は、伝えられた戦略に関する知識を被告らが自己の利益のために使用することは認められないとの判断を示した。被告は、裁判所の差止命令により、原告の会社の営業秘密のさらなる持ち出しを禁じられた。

(6)　　著作権侵害

いくつかの事例において、複数の裁判所が、利用のためデータベースに格納されている顧客データは、法の下で営業秘密だと認定している。また、コンピュータデータベースを含む編集物は、1957年著作権法第２条（o）に従い「文学的著作物」と見なされる。

編集物に関わるGovindan対Gopalakrishna訴訟判決（AIR 1955 Mad 391）では、編集物が独自の内容をほとんど含まない場合でも、法的に保護されるとの判断が示された。したがって、そのような編集物の場合についても、いかなる企業も従業員の思考、スキル、労働の成果を窃取又は侵害する権利はない。

(7)　2000年情報技術法（IT法）

IT法は、特定のケースにおいて国外にも適用される。例えば、インド国内に物理的に立地するコンピュータシステムに対し、インド国外からサイバー攻撃が行われ、その結果、営業秘密が不正利用された場合、IT法によれば当該サイバー攻撃はインド国内での訴追対象となり、関連する法執行当局には、法的措置を講じる権限が認められることとなる。

(8)　訴訟の提起先

営業秘密に関する民事上の紛争については、（訴訟提起のための）裁判所の管轄権は、民事訴訟法（CPC）第20条に従い決定される。民事訴訟は、被告がその管轄区域内に居住するか事業を営み、又は利得を求めて個人的に活動している地の裁判所、又は管轄区域内で訴訟原因が発生した（全部であるか一部であるかを問わない）裁判所に提起されるものとする。さらに、事案の金銭に関わる裁判所の管轄権もまた、訴訟をどの裁判所に提起すべきかを決定する際に重要となる。

(9)　訴状における営業秘密の記載法

訴状は、被告側により細部まで読まれることとなるため、営業秘密の機密性を損なうことなく、訴状内で営業秘密をどの程度開示すべきかの判断は、多くの場合、複雑な作業となる。

重要なのは、Bombay Dyeing and Manufacturing Co Ltd対Mehar Karan Singh訴訟判決（2010（112）Bom LR 375）で示された以下の基準に基づき、当該情報が営業秘密であると認定されるに足る十分な開示でなければならないということだ。

(i)　当該情報がその企業の外部で知られている度合
(ii)　当該情報がその企業の内部、すなわち従業員に知られている度合
(iii)　当該営業秘密の機密性を守るために保有者が講じた対策
(iv)　競合他社が本来は保有していない当該情報を有していることにより得られる利潤及び保有者にとっての価値
(v)　当該情報の入手及び開発に要した労力又は費用

(vi) 他者が当該情報を取得し、複製するのに要するであろう時間及び費用

原告は、訴訟で勝訴するために、訴状に以下の側面を含めることもできる。これは、裁判所に営業秘密の価値とその技術的側面を明確に説明し、裁判所に暫定的な差止命令、そして最終的には損害賠償を認めるよう説得するのに役立つ。この方法で情報を提示すると、成功の可能性が高まる。

(i) 製品の成功への貢献という点における当該営業秘密の重要性及び当該営業秘密により競合他社に比して会社にもたらされる競争優位性。
(ii) 訴状には、当該営業秘密の裏付け/参照なしに技術的営業秘密をリバースエンジニアリングすることは不可能であることを示す詳細も含める必要がある。
(iii) 必要に応じ、営業秘密の説明は開封できないように封印の上、提出し、両当事者が当該情報を公開できないよう、機密保持クラブ（confidentiality club）の形成の要請を行うことができる。

(10) 営業秘密の不正利用に関する民事訴訟における暫定的又は終局的な差止命令

インドでは、訴訟の予備段階及び最終段階において、原告又は権利保有者が、被告による営業秘密の使用又は開示を差止めることができる。

Gujarat Bottling Co Ltd 対 Coca Cola Co 訴訟判決（(1995) 5 SCC 545）において、裁判所は、裁判所の判断により差止命令を出すための条件について以下のとおり判示した。

(i) 反証が出されなければ事実を証明するのに十分である一応の証拠を原告が提示したか
(ii) 比較衡量の結果、原告に有利であるか否か
(iii) 差止命令が出されなかった場合、原告が回復不可能な損害を被るか否か

また裁判所は、仮差止命令の目的について、営業秘密による損害が損害賠償によっては十分に補償されない場合、その損害から原告を保護することであると判示している。この考え方は、情報の価値がその秘密性に由来する営業秘密については特に当てはまる。

したがって、このような原告を保護する必要性は、被告がその法律上の権能を行使することを妨げられることから被る損害・不利益と比較検討されなければならない。

原告は、上記の各要件を満たすためことを示すため、審理の冒頭で、法的措置を求める対象となった営業秘密がどのようなものか明確にしなければならない（詳細は説明しない場合であっても。）。原告はまた、営業秘密の商業的価値及び原告にとってその重要性を示す事実を主張しなければならない。当該営業秘密がもたらす競争上の優位性に関する説明もまた重要なものとなる。当該営業秘密が利用された際の性質及び程度は、規模及び期間の双方において、被り得る損害と同様に、比較衡量を決定するために重要である。ここでいう性質とは、侵害者が「企業秘密」の利点を得るためにどのように企業秘密を利用するかを意味する。裁判所が仮差止の救済の申請を検討する際に考慮する要素の 1 つは、差止命令を認めないことが原告に多大な損失と損害を与えるかどうかである。したがって、仮差止命令は認められなければならない。これは一般に便宜均衡と呼ばれるもので、原告が確立するものである。　したがって、「営業秘密の使用の性質」が重要になる。

（11）　雇用主と従業員の関係

雇用主と従業員との間の雇用関係に関連する事案では、追加的に 1857 年インド契約法第 27 条が検討される必要がある。取引（あらゆるビジネス又はサービスを意味する。この文では、個人のビジネス又は雇用の追求を制限するような制限は法的強制力がないことを伝えようとしている）を禁止するあらゆる契約又は条件は、一般論として、本規定に基づき無効かつ強制不能とされる。したがって、原告が雇用主であり、雇用契約における秘密保持条項に基づいて、従業員が競合他社へ転職することを禁止している場合、そのような条件は強制することができない。一方で、競合他社のために同じプロジェクトに従事したり、同じ製品を開発しないよう義務付ける条件は、強制可能である。

（12）　営業秘密の侵害に対する損害賠償

（i）　訴訟当事者は、営業秘密の不正利用に対する救済として、損害賠償及び利益の返還を求めることができる。損害とは原告にとっての実際の潜在的な損失を意味し、一方、利益の返還は被告が得た利益を指す。損害は、裁判所による判決がなされる前に、算定及び証明する必要がある。損害賠償額には、予定損害賠償額、実質的損害賠償額又は懲罰的損害賠償額が含まれる。

（ii）　具体的に金額が算定されていない場合、予定損害賠償額は、両当事者間での契約条件に基づく金額の算定が求められることとなる。

（iii）　実質的損害賠償額は、証拠を通じて証明されなければならない（これに関連し、証人が反対尋問を受ける場合もある。）。この額は、営業秘密の開示によって生じる損失の算定、又は営業秘密自体の想定市場価値に基づく評価となる可能性が高い。この額は、専門家の報告書により裏付けることもできる。

(iv) 懲罰的損害賠償額は、通常、裁判所の権限及び裁量に基づくものであり、侵害又は不法行為が重大な場合に認められる。懲罰的損害賠償は通常、裁判所の特権と裁量に基づいており、侵害又は不法行為がひどい場合に認められる。被告が不法行為をしており、常習的、意図的に、原告に損害を与える方法で原告の登録された知的財産権を侵害していることが判明した場合、原告は懲罰的損害賠償を請求することができる。デリー高等裁判所は、Koninlijke Philips NV & Anr 対 Amazestore & Ors 訴訟判決において画期的な判決を下し、知的財産権侵害に関する訴訟で損害賠償を与える際に従うべき基本原則を定めた。この訴訟の原告は、侵害製品の販売価格、被告が侵害製品を販売した際の利益率、侵害製品の原価、各侵害製品の販売で被告が得た利益（1 個あたり）、合計数、侵害製品の種類と、侵害製品が市場に出回ってからの期間に基づき損害を計算した。裁判所はまた民事訴訟における被告の違法行為の程度が、裁判所が原告に与える救済の性質を決定することが多いと考えた。裁判所は、不法行為の程度が、実際の損害賠償請求に加えて認められる損害賠償の金額と性質に直接影響を与えるとの見解を示した。たとえば Time Incorporated 対 Lokesh Srivastava 訴訟判決では、裁判所は、侵害に対する懲罰的損害賠償として 500,000 ルピーの支払を命じ、原告に対する評判と信用の喪失に対する追加の補償的損害賠償として 500,000 ルピーの支払いを命じた。同様に、Yahoo Inc v Rinshad Rinu & Ors 事件では、懲罰的賠償額は、補償損害賠償額の 1.5 倍、それぞれ 300,000 ルピー及び 200,000 ルピーであった。

差止命令及び損害賠償とは別に、原告又は営業秘密保有者に認められ得るその他の民事上の救済には、営業秘密を含む資料（例：紙資料や USB 等の情報を記録した記録媒体、金型等の情報を化体した物件）の返還・引き渡しを認める命令、及び被告が不正利用した資料の保管（損害賠償額算定のための資料として）のための裁判所委員の任命などがある。裁判所は、裁判所委員が裁判所による適切な捜索・差押命令を遂行するに当たり、地域の警察に対しこれを補佐するよう指示することもできる。

(13) 刑事上の救済

1860 年インド刑法及び 1957 年著作権法（著作権を保護）、2000 年情報技術法（電磁的記録を規律）など特定のテーマに関する法律には、禁錮刑又は罰金刑に処せられる可能性のある犯罪を具体的に定める条項が含まれている。ただし、営業秘密の不正利用を犯罪として具体的に挙げている条項はない。なお、事案によっては、背任罪、窃盗罪、詐欺罪等の罪が適用される場合がある。

背任罪に対する刑罰は、３年以下の禁錮又は罰金である。委託を受けた財産を不正に流用し、又は自己の使用のために換金し、又は（明示的か黙示的かを問わず）契約又は準拠法に違反して不正に使用又は処分し、又はその他の者にこれを許した場合、その者は背任罪を犯したものと見なされる。これにより、告訴人は、まず、権利侵害者又は被告人が不正な意図をもって財産の不正利用、換金、使用又は処分を行ったことを立証しなければならない。

刑事訴訟に関する手続は、1973 年刑事訴訟法に規定されている。犯罪は告訴により警察に通知することができる。当該犯罪がインド刑法で規定された違法行為である場合（３年を超える禁錮刑が科される）、警察官は、犯罪被害証明書（First Information Report）を登録しなければならず、また、令状なしに捜査を開始し逮捕することができる。しかし、当該犯罪がインド刑法で規定されていない場合には、警察には捜査開始の義務はなく、捜査はすべて治安判事の命令に基づき行わなければならない。この治安判事は、まず刑事告訴を評価し、必要に応じ捜査、逮捕等を命じる。

インドの刑事司法機関では遅延が問題化しているため、違反行為が悪質であり、捜査やそれに付随する刑罰を求めるだけの意味があるなど戦略的に有益である場合、又は犯人の身元が不明で捜査の必要がある場合を除き、営業秘密保有者にとって好ましい執行の選択肢ではない。

(14)　訴訟手続の営業秘密の保持

インドの裁判所は、営業秘密を第三者や他方の訴訟当事者の目に触れさせないようするために、訴訟当事者が様々な措置を講じることを認めている。このような措置のうち主流となっているものは、封印された表紙を付して情報を提出するという慣行であり、裁判官のみがその内容を確認できる[17]。また、比較的新しい慣行として、営業秘密情報が秘密保持契約の下で限られた数の者にのみ閲覧可能にする[18]とともに、営業秘密情報の確認又は営業秘密情報に関する弁論を（法廷に第三者・傍聴人を入れずに）

[17] 日本の不正競争防止法でも、営業秘密が記載された文書は文書提出命令の対象から除外される正当な理由の有無（営業秘密が記載されているか否か）について、事前に裁判官のみが審理（確認）することができるとするいわゆる「インカメラ審理」の規定がある（第 7 条）。

[18] 日本の不正競争防止法でも、営業秘密が記載された文書が訴訟当事者から証拠として提出された場合に、相手方に対して訴訟追行の目的以外で使用・開示してはならない旨を裁判所が命じることができ（第 10 条・秘密保持命令。なお、違反には刑事罰あり。）、秘密保持命令が発せられた訴訟の訴訟記録については閲覧が制限することができるとの規定がある（第 12 条、民事訴訟法第 92 条）。

非公開で行われる[19]ように図る「機密保持クラブ」がある。

(15)　その他の紛争解決手続

2015 年商事裁判所法第 12 条（A）に基づき、デリー高等裁判所の仲裁・調停センターに訴訟前調停を申請することができる。このような手続は、和解の可能性が高い場合に有効である。さらに、当該手続におけるすべての協議は、機密とされ、他の救済手段を損なうことなく実施される。

仲裁条項を含む契約では、紛争が生じた場合、いずれの当事者も、1996 年仲裁調停法第９条及び/又は第 17 条に基づく仮差止命令を求めることができる。

[19] 日本の不正競争防止法でも、営業秘密に該当する事項について当事者が尋問を受ける場合には、裁判所は、裁判を公開しないで行うことができるとの規定がある（第 13 条）。

6. 近年の訴訟動向

営業秘密に関するいくつかの重要な訴訟判決及びその解説（民事救済及び/又は刑事制裁、及び/又は行政上・多国間の措置等)。

以下は、様々な状況下でインドの裁判所により下された営業秘密に関する顕著な判例である。

(1) 営業秘密の定義に関する判例

Saltman Engineering Co. 対 Campbell Engineering Co. Ltd.裁判における控訴裁判所判決は、保有者と受領者との間で共有された情報が実際に機密であるかどうかを決定するため、インドの多くの裁判所が判例とする重要な判決である。本件では、同裁判所は、機密情報は「公共の財産又は公共の知識であってはならない。」と判示した。一方、裁判所は、「誰もが利用可能な素材上に作成者が作業した成果である、製品構造、計画、スケッチ、又はそれらと同種のものが機密情報である可能性は十分にあり得る。文書の作成者が自身の頭脳を用い、その結果、同じプロセスを経ることによってのみ他者が生み出すことができる結果を生み出したという事実が、それらを機密たらしめる。」と判示した。

ここで、「知られた秘密ではない情報」(information to be known or not secret)とは、インターネットなどのオンライン又は市場などのオフライン媒体を通じて公衆に入手可能な情報であり、「パブリックドメイン」(public domain) 及び「公共財産(public property)又は公共知識(public knowledge)」とされるものもある。これらの用語はすべて同じ意味である。

同様に、デリー高等裁判所は、2005 年の Ambience India Pvt. Ltd 対 Shri Naveen Jain 訴訟判決において、「営業秘密は保護された機密情報であり、従業員が雇用期間中に取得したとしても、雇用主の利益のため、他者に引き渡してはならない。しかし、多くの者が認識し、他者から広く知られている雇用主の日々の業務内容は営業秘密と呼ぶことはできない。」と判示した。

同様に、Fairfest 訴訟 (2015 年)、Diljeet Titus 対 Alfred A Adebare and Ors 訴訟 (2006 年)、Hi-Tech Systems 及び Services Ltd 対 Suprabhat Ray and Ors 訴訟 (2015 年)、Burlington Home Shopping Pvt. Ltd 対 Rajnish Chibber 訴訟 (1995 年) においてカルカッタ高等裁判所は、営業秘密の保有者によって然るべく保護され、開示されれば保有者に損害を与える可能性のある情報は、営業秘密又は機密情報として取り扱われるべきことを明確に定めている。同判決では、営業秘密には、製法、技術的ノウハウ、他者が知ることなく雇用主が採用する特殊な事業の形態や手法も含まれるとしている。また、営業秘密にはジョイント・ベンチャー契約、ローン契約、クライアントリスト、クライアントに関連した開示契約も含まれる。金銭貸借契約、顧客リスト、費用や価格などの事業関連情報、設備投資計画、在庫販売戦略もまた、営業

秘密に分類される。Burlington Home Shopping 訴訟では、クライアントデータベースの著作権侵害が主要論点とされていたが、収集されたデータベースが営業秘密保護の適用対象となることも強調された。

以上のとおり、インドでは、他者が容易に入手できず、秘密に保持されていることから商業的価値を有し、その保護のために保有者が措置を講じている限りにおいて、企業情報、産業情報、技術ノウハウ、又は工程といったカテゴリーに属する広範な情報を営業情報として保護の対象としている。

(2)　雇用主と従業員との間の営業秘密に関する判例

当該テーマに関する判例は、秘密保持及び競業避止契約はインドの裁判所により支持されているものの、契約中のこれらの制限的条項の合理性が重要な検討事項とされていることを示している。

契約における制限的条項の合理性に関する問題は、1967 年 1 月 17 日の Niranjan Shankar Golikari 対 Century Spinning and Mfg Co. Ltd.訴訟判決（1967 AIR 1098, 1967 SCR (2) 378）の中でインド最高裁判所において判断された。インド最高裁判所は、雇用契約期間中に効力を有する、negative covenants（一定の行為を行わない約束・義務）は、一般的には取引を禁止するものとは見なされないと判示した。また、従業員が同業他社や他企業に雇用されず、自ら事業を立ち上げず、類似又は実質的に同様の職務を遂行しないという negative covenants は、当該契約が不当、過度に過酷、不合理又は一方的なものでない限り、取引禁止には当たらないとしている。この場合、契約書中の制限は合理的なものであり、取引禁止には当たらないとの判断を示した。

特に従業員が懸念する場合には、negative covenants を注意深く定める必要性について、デリー高等裁判所は、1979 年 7 月 20 日の Superintendence Company of India (P) Ltd 対 Sh Krishan Murgai 訴訟判決（AIR 1979 Delhi 232）において、雇用契約に関し、従業員と雇用主の交渉力には本質的に不均衡があるため、雇用時に従業員が契約の実体的な内容について深く考慮しない場合があるとした。同裁判所は、禁止措置は「雇用主を保護するための必要性を超えたものであってはならず、また、不当に過酷又は従業員を圧迫するものであってはならない。」としている。したがって、雇用契約の終了後、従業員が雇用主の事業に類似又は競合する事業に従事しないことを要求する広範な negative covenants について、同裁判所は、それが従業員が生計を維持する上で不当な影響を及ぼすことを理由として、認められないと判断した。

同時に、同裁判所は、従業員が自らに委ねられた営業秘密又は機密情報を、自身の事業又は職務において自らを利するための「きっかけ」として利用することについて

は厳しい見方を示した。カルカッタ高等裁判所は、2015 年６月 17 日の Hi-tech systems and Services Ltd 対 Suprabhat Roy and Ors 訴訟判決（G.A.1738 of 2014 及び C.S.192 of 2014）において、被告が原告から雇用されている間に取得した機密情報を基に、被告が原告の顧客に取引を勧誘しているとした。これを受け、同裁判所は、既存契約の侵害は原告に衡平法上の救済を与えるものであることを理由に、被告に対し、原告が第三者との間に結んだ既存契約の一切の侵害を禁ずる差止命令を出した。

同様に、Niranjan Shankar Golikari 対 The Century Spinning And Mfg. Co.訴訟判決（1967 AIR 1098, 1967 SCR (2) 378）において、最高裁判所は、一審判決及び高等裁判所による判決を支持し、専門的な情報を競合会社に開示することは被告の利益を害するものであり、「時期、雇用の性質及び地域についての制限であり、被告である会社の利益保護の観点からは、広範、不合理又は不必要であるとは言えない。」として、上訴人（原告）に対する差止命令を認めた。

(3)　ベンダーと購買企業との間など、企業間の契約を通じて共有される営業秘密に関する判例

ベンダーと購買企業との間の契約やパートナーシップ契約のような企業間の契約の場合、裁判所は、制限的条項について、より制限が少なく、より好意的な見方を示してきた。

1995 年８月４日の M/s Gujarat Bottling Co. Ltd（GBC）and Ors 対 Coca Cola and Ors 訴訟判決（1995 AIR 2372, 1995 SCC (5) 545）において、最高裁判所は、1993 年に両当事者間で締結された契約は、GBC が飲料を製造、瓶詰、販売及び流通することを認める一方で、GBC が競合商品を取り扱う権利を制限したフランチャイズ契約であるとした。裁判所の判断は、当該の negative covenants は、フランチャイザー製品の流通促進のためのものであり、取引の禁止とは見なされないというものであった。また、その後の Coca Cola に情報を提供しないまま GBC が Pepsico Ltd に自社株を譲渡した行為は、1993 年に締結された契約に違反したものであり、同社は Coca Cola との取引において不公正かつ不公平な行為に及んだとした。これを受け、同裁判所は、「1996 年１月 25 日までの間、アーメダーバード及びラージコートの工場を使用し、それが何者であるかにかかわらず他者の飲料を製造、瓶詰、販売又は取引する、又は何らかの方法で関与することを禁じた高等裁判所による差止命令には、いかなる瑕疵も見当たらない。」との判断を示した。

カルカッタ高等裁判所での Fairfest Media Ltd 対 ITE Group Plc 訴訟（GA No.3174 of 2014 及び CS No.329 of 2014）では、原告は被告との間で、両者間で検討されていた合弁契約に先立ち、秘密保持契約（NDA）を締結していた。この NDA は、署名日であ

る2013年３月15日から６ヶ月間有効であった。当該NDA締結後、被告の要請により、原告は財務・販売に関する機密情報を伝えた。しかしながら、2014 年４月に合弁契約案は被告により撤回された。被告は機密情報すべてを入手していたが、原告・被告の両者間で締結された NDA もまた無効となった。同裁判所は、衡平法の原則及びスプリングボード・ドクトリン（守秘を条件に入手した情報を、入手先に損害を与える形で自らを利するために使用してはならないという考え方）[20]に基づき本件を審理し、特に、提案された旅行見本市に関連して原告から受領した販売戦略、顧客基盤に関する情報を被告が共有することを禁止した。

(4)　契約上の合意が存在しない場合の営業秘密の保護

当該状況に関連する重要判決の一つが、デリー高等裁判所による 1987 年７月６日の John Richard Brady 対 Chemical Process Equipments 訴訟判決 *(AIR 1987 Delhi 372)* である。本件では、被告らは、原告から飼料生産ユニットの図面を、工場内で必要な特定のパーツを提供するという限定的な目的のためとして入手していた。しかし、被告らは情報を不正利用し、飼料ビジネスに参入するための「きっかけ」として使用していたことが判明した。デリー高等裁判所は、審理に当たり、情報が秘密である限りにおいて、開示及び不正利用からそれを保護する正式契約の有無は大きな問題ではないとした Saltman 訴訟における Greene 判事による判示に依拠とした。同裁判所は、被告らが保有する情報を利用することを禁じ、一般的な衡平法の原則及び守秘義務違反を理由として、費用の支払を科した。事実審理に当たり、同裁判所は、機密情報に関連した紛争において利用可能となるべき救済について、Saltman 訴訟における Greene 判事の判示に触れた。Greene 判事は、３つの状況に分けてこれを整理・分析し、まず、契約が存在し、一方の当事者が機密情報を受け取った場合、契約中に明記されていなくとも、情報を秘密に保持する義務が受領した側の当事者にあるとした。次に、明示的か黙示的かを問わず同意を得ないまま、直接的又は間接的に原告から取得した機密情報を被告が使用したという状況においては、被告は原告の権利を侵害した罪に問われるとした。さらに別の状況として、情報が秘密である限りにおいて、契約の存在有無にかかわらず、情報を受領した側の当事者に義務が発生するとした。

デリー高等裁判所による 1998 年 10 月 16 日の Escorts Construction Equipment Ltd 対 Action Equipment P. Ltd 訴訟判決（IA No. 2460 及び 4638/98）は、重要な役職に 10 年近く在籍した元従業員が、退職後３年以内に原告が製造していたピックアンドキャリー自走式クレーンと極めて類似した製品の製造会社を設立した事案についてのも

[20] この考え方の詳細については、以下を参照。
https://www.legalserviceindia.com/legal/article-3780-spring-board-doctrine-a-critical-study-of-trade-secret-protection.html

のである。契約上の違反行為はなかった。しかし、デリー高等裁判所は、原告の従業員であった被告が元の雇用主の意匠を不正利用しようとしたとして、守秘義務違反を理由に差止命令を出した。被告が仮差止命令により制限を受けない限り、金銭的に見積もることのできない回復不可能な損失又は損害が生じかねないため、比較衡量は原告に有利なものとなるとの判断が示された。

カルナータカ高等裁判所は、2005年10月20日のV.V. Sivaram and Ors 対 Foseco India Limited訴訟判決（2006 133 CompCas 160 Kar, 2006 (1) KarLJ 386）において、12 年近くにわたり原告企業に勤務した後に退職した被告らが、機密ノウハウを保有し、これを原告の製品と似た製品を製造するために使用し、また、原告の製品だと偽ろうとしたとして、守秘義務違反を理由に被告（本件では控訴人）に対し一審が出した差止命令を認めた。同裁判所は、原告の権利を保護する黙示の義務は強制可能であるという事実を認め、さらに、従業員による雇用終了後の機密情報の開示を禁止することは可能であるとした。

(5)　第三者により情報が盗まれた場合の営業秘密の保護

カルナータカ高等裁判所は、2012年10月10日のHomag India Private Ltd対Ulfath Ali Khan訴訟判決（M.F.A.No.1682/2010 C/W M.F.A.No.1683/2010 (CPC)）において、第一被告は、第二被告であるM/s IMA Klessmann GmbHから守秘義務に違反するよう唆され、自身の Homag メールアドレスから個人用メールアドレスに機密データを送ったことは書証により一応に立証されたと判示した。さらに、「当該状況下では、原告は、第二被告が原告の営業秘密情報を利用して第二被告の事業の成長を図ったことを立証する必要はない。」と判示し、守秘義務違反及び機密情報の不正使用は提訴可能な権利であるとの判断を示した。被告らは、仮差止命令により、業務継続、原告の顧客との取引、また、技術データ、製造工程、販売計画、販促、価格、顧客リスト、ソフトウェア、仕様書、技術的手法等の情報の利用を禁止された。

以下は、インドの裁判所により下された営業秘密に関するその他の重要な判例である。

①Bombay Dyeing及びManufacturing Co Ltd対Mehar Karan Singh訴訟判決（2010 (112) Bom LR 375）

○事案の概要

(i)　本件において、原告はWADIAという企業の所有者であり、被告は当該企業の取締役に任命されていた。

（ii） 被告は、原告の求めに応じ、在職中又はその後に機密情報を漏らしてはならないという書面に署名し、その遵守を約した。
（iii） その後、原告との雇用継続中に、被告が DD（原告の競合企業）に取締役として入社していたことが判明した。
（iv） さらに、原告が対価を支払いソフトウェアメーカーOracle から取得した、原告の不動産業務用カスタマイズソフトウェアのマニュアル等を被告がメールで転送し、競合他社 DD に機密情報を漏洩したと原告は主張した。

○争点

（i） 原告のカスタマイズソフトウェアのマニュアルを被告が競合他社と共有することは、機密情報の開示に相当するか。
（ii） 被告による機密情報の漏洩・開示に対して、原告が求める差止請求は認められるべきか。

本件において、ボンベイ高等裁判所は、営業秘密であるかを判断するため、以下を検討した。

（i） 当該情報がその企業の外部で知られている度合
（ii） 当該情報がその企業内部の者に知られている度合。すなわち、当該営業秘密の保有者が秘密を守るために講じた対策
（iii） 競合他社が保有していない当該情報を有していることにより得られる利潤及び保有者にとっての価値
（iv） 当該情報の入手及び開発に要した労力又は費用
（v） 他者が当該情報を取得し、複製するのに要するであろう時間及び費用

○裁判所の判断
（i） 被告は、被告の電子メールに添付されたソフトウェアマニュアル中の機密情報を、いかなる方法であれ、他者や他企業、又は原告の競合企業に漏洩又は引き渡してはならず、また、自己の使用のために、いかなる形であれ、これを利用してはならない。
（ii） 同裁判所は、「営業秘密」の定義を検討するため、Black’s Law Dictionary（第８版）の 1533 ページ及び Pollock と Mulla の手になる契約法に関する権威ある解説書（第 13 版）838 ページを参照し、次のような判断を示した。
・従業員が記憶する情報は、契約期間満了後又は当該従業員のその後の事業において、当該従業員が使用できる。
・従業員が複写する権限がない、顧客リストを含むすべての機密情報は、雇

用主に不利益を与える形で当該従業員が使用することはできない。これは、従業員が、雇用期間中に知り得た営業秘密又は機密情報を、他者に開示したり又は自己の利益のために使用したりしないという雇用主に対する忠実義務によるものである。

(iii) さらに、同裁判所は、情報を営業秘密と認定するための以下の要素を検討した。

・当該情報がその企業の外部で知られている度合
・当該情報がその企業の内部、すなわち従業員により知られている度合
・当該営業秘密の機密を守るために保有者が講じた対策
・競合他社が保有していない当該情報を有していることにより得られる利潤及び保有者にとっての価値
・当該情報の入手及び開発に要した労力又は費用
・他者が当該情報を取得し、複製するのに要するであろう時間及び費用

(iv) また、同裁判所は、営業秘密の原則においては、新規性や用途は認定に求められる要素ではないと判示し、コンピュータソフトウェアは、一般的な営業秘密関連法及び原則の下で保護されるとした。

(v) 本件において、原告はソフトウェア開発に9年を要しており、これを被告は100万ドル近い額と引き換えにDDに共有していた。

(vi) 判決理由において、契約で定められている場合を除き、ある情報が機密とされるためには、当該情報についての機密性の要件を備えていなければならず、かつ、公共の財産又は公共知識であってはならない。

(vii) 被告は、被告の電子メールに添付されたソフトウェアマニュアル中の機密情報を、いかなる方法であれ、他者や他企業、又は原告の競合企業に漏洩又は引き渡してはならず、また、自己の使用のために、いかなる形であれ、これを利用してはならないと、同裁判所は特記した。

②デリー高等裁判所による1987年7月6日のJohn Richard Brady対Chemical Process Equipments (P) Ltd.訴訟判決 (AIR 1987 Delhi 372)

○事案

(i) 原告は、屋外の気象条件にかかわらず、一年を通じて牧草を生産することのできるコンパクトな機械ユニット内で、家畜の食料である新鮮な緑草を栽培するというアイデアを思いついた。

(ii) 原告は、1972 年に独自の飼料生産ユニット（以下「FPU」）を開発し、インドにおいて国内向け及び輸出向けの FPU の製造を開始することを決定し、被告が製造した感熱パネルの調達検討のため、被告に見積もりを依頼した。

(iii) 被告が見積もりを作成送付できるよう、原告は被告に対し、FPU に関するすべての技術資料、詳細なノウハウ、図面、仕様書を、秘密保持契約を締結した上で共有した。被告は、この契約が有効である間、被告がこの感熱パネルを原告以外の者のために製造しないこと、また、提供された詳細及び仕様書を漏洩しないことに合意した。

(iv) その一方で、被告は、FPU のオペレーションノウハウ及び技術を知るため、原告の FPU が稼動している地域を何度にもわたり訪問したとされる。

(v) その後、原告は、原告の FPU に偽って見せかけたと思われる機械を被告が考案したことを知った。

(vi) これらの状況を考え合わせ、原告は、被告が秘密保持契約の下で開示された原告のノウハウ、情報、図面、意匠、仕様書を不正に改変し不正利用したことにより、守秘義務に違反したと主張した。

(vii) 上記に関し、被告は、自分たちは著作権を侵害しておらず、また、当該契約への一切の条項に関し、違反の責を負うものではないと主張した。また、被告は、海外市場では長年にわたり、同様の機械を製造する企業が存在すると申し立てた。被告は、FPU に関する図面、技術資料、ノウハウを原告が提供したことを否定した。

○争点

(i) 被告が著作権を侵害したか、あるいは被告が秘密保持契約のいずれかの条項に違反しているかどうか。

(ii) 原告が主張するように、被告が守秘義務に違反したかどうか。

○裁判所の判断

(i) 裁判所は、両当事者の機械が酷似しているとの判断を示した。

(ii) さらに、被告は原告の図面を入手してもいた。裁判所はまた、被告が実際にどのようにして被告の機械を考案したかについて明らかにしていないとした。

(iii) 原告は、その著作権が侵害されたこと、及び厳格な守秘義務の下で当該 FPU に関する仕様書、図面、その他の技術的情報が被告に提供されたことについての強力な一応の立証を行ったとの判断を裁判所は示した。

(iv) 裁判所は、被告は、自身に委ねられた原告の FPU に関するノウハウ、仕様書、図面その他の技術的情報を、市場参入のための「きっかけとして使用して原告に損害を与えており、被告がこれらの情報を濫用することを禁ずることは公正の原則に適うとの明確な判断を示した。

(v) これを受け、裁判所は被告に対し、原告の FPU の図面を実質的に模倣・複製した機械の製造及び販売、並びに原告が当該 FPU について被告に開示したノウハウ、仕様書、図面その他の技術的情報を、他のいかなる形であろうとも使用することを禁止した。

(vi) 同裁判所は、契約書中に明示的な秘密保持条項がなくとも、秘密保持は黙示されており、被告は守秘義務違反の責任を負うとの見方を示した。

③カルカッタ高等裁判所による 2015 年６月 17 日の Hi-Tech Systems 対 Suprabhat Ray 訴訟判決（G.A.1738 of 2014, C.S.192 of 2014 及び AIR 2015 Cal 261）

○事案

(i) 原告企業は過去に被告らを雇用しており、被告らは、雇用中に回付された行動規範及び方針に基づき、その雇用期間中及び雇用終了の日から３年間、提供されたすべての情報及び資料を機密に保持することを義務付けられていた。

(ii) 被告らの退職後間もなく、原告は、被告らが競合企業を立ち上げ、原告のデータベースから不正に入手した貴重なデータ及び情報を用いて、原告の顧客に売り込みを図っていることを知った。

(iii) そのため、原告はカルカッタ高等裁判所に対し、機密情報及び営業秘密を含む原告のコンピュータデータベースを、いかなる形であろうとも漏洩及び/又は使用することを被告に禁ずる差止命令を求め提訴した。

○争点

(i) 本件は、勧誘禁止、競合避止及び守秘という三つの問題に関わるものであり、特に、（原告の元従業員としての）被告が、原告と直接競合する取引に従事し得るか、また、かかる取引の過程で、その雇用の過程で入手した営業秘密及び機密情報を利用できるか否かを問うものである。

○裁判所の判断

(i) 同裁判所は、被告らに対し、前述の行動規範及び人事方針に規定された通り、退職/雇用期間終了後の３年間、原告の営業秘密及び機密情報の利用並びに原告の顧客の販売代理人としての活動を禁じた。

(ii) 同裁判所は、被告が原告と同一又は類似の事業を営むことを裁判所命令により妨げられるものではないとしたが、事業遂行においては原告のデータベース及び営業秘密を使用又は利用せずにこれを行うことを条件とし、原告の営業秘密を保護した。

(6) 上述の営業秘密関連訴訟における近年の判例の傾向

インドには営業秘密保護に関する特別な法令は存在しないが、判例の分析からは、営業秘密の定義、多くの保護救済、裁判所において不可避となる開示という関連課題などの重要テーマを含む営業秘密に関する広範かつ増え続ける判例の存在がうかがうことができる。2000 年情報技術法の公布及び電子的ルートにおける機密情報の窃取並びに厳格な罰則、損害賠償及び禁錮刑について定めたその後の法改正が示すように、技術革新に対応するため、法制度は大きく変化してきた。重大犯罪に対する刑事上の制裁措置（罰則）についても、刑事訴訟法第 405 条から第 409 条及び第 418 条において規定されている。重大犯罪とは、逮捕保釈が権利の問題ではないケースを言う。 重大犯罪とは、3 年以上の禁錮に処される犯罪を言う。

第 2 章 －営業秘密の漏洩に対する実践的対策（以下を含む）－

（i） 社内における営業秘密の管理方法
（ii） 社外における営業秘密の管理方法
（iii） 国外に営業秘密を持ち出す際の留意事項
（iv） 営業秘密の公証を最大限活かすには
（v） 「優れた」契約を締結するには
（vi） 営業秘密保護のための管理体制を構築するには
（vii） 在宅勤務時の営業秘密保護に当たっての留意事項

以下では、営業秘密の社内外での管理方法についての推奨事項を挙げている。同様の方策は、社外又は国外において営業秘密を管理する場合にも用いることができる。

さまざまな組織が直面している主要課題の一つは、近年技術が進歩し、オンラインでの情報の共有・コピー・保存が容易となる中で、自社の機密情報をいかに保護するかである。

営業秘密の保護対象となるような情報を保有する企業は、当該情報が開示されないようにするため、以下に述べるような一定の措置を講じることが求められる。

（i）営業秘密として保護されるべき情報の正確な範囲及び性質の特定
保護されるべき各情報を特定し、新規作成資料のうち秘密に保持されるべきものを特定する仕組みを構築する。
（ii）適切な営業秘密方針の策定
営業秘密を取り扱うすべての従業員は、秘密情報の保護及び適切な取り扱いに関し、研修を受講し、秘密保持契約（NDA）及び会社方針に署名しなければならない。
(iii)営業秘密情報へのアクセスの制限
関係者以外の見学を制限し、すべての訪問者に入館時の入館手続を義務付ける。営業秘密情報を含む、又は営業秘密が記載されている文書には、「極秘」と必ず表示する。これらの文書の複写及び配布を制限し、必要に応じて複写には附番し、必ず文書の持ち出し記録を付けさせるようにする。
(iv)必要に応じて守秘義務契約及び NDA を締結する
すべての従業員が守秘義務契約及び NDA に署名することが重要である。企業は、当該企業を退職する従業員に対し、営業秘密資料の返却を要求し、NDA の存在を再確認させる退職時監査を実施すべきである。

営業秘密の保有者が、技術移転契約又はその他のライセンス契約に、移転された技術は機密性のあるものであり、ライセンシーは、その契約期間中及び契約終了後も守秘義務を負う旨を記載した条項を含めることは、合理的措置である。

さらに、保有者は、ライセンシーに対し、当該ライセンシーの従業員、下請業者及び工場訪問者との間で、秘密保持のために適切な秘密保持契約を締結するよう義務付けるべきであろう。営業秘密の保有者はまた、すべての技術マニュアルに、その中に含まれる情報が専有情報でありかつ秘密性を有することを明記した注意書きを挿入すべきでもあろう。

営業秘密の保有者は、営業秘密の開示を防止するため、物理的、技術的、アクセス管理上及び契約上の措置を講じなければならない。以下は、営業秘密の漏洩を防止するための具体的な対策である。

(1) 守秘義務契約／NDA

守秘義務契約は／NDA、新入社員の入社時又は従業員の退職時や、業務提携の際等、様々な状況下において、両当事者間で署名すべきものである。多くの状況において、インドの裁判所は、守秘義務契約が営業秘密の保有者の利益を保護するためには不可欠だと合理的に見なされる場合、秘密保持契約は履行強制可能であると判断してきた。

以下のような状況下において企業は NDA への署名を求めることができる。

(i)一部の企業は、新入社員が入社する際及び従業員が退社する際、NDA への署名を義務付けている。一部の企業では、すべての従業員に NDA への署名を義務付けているが、それ以外の企業では、選択された部門又は種類の従業員のみが契約の対象としている。

(ii)また、複数の企業間の交渉の冒頭段階で NDA は締結される。これは両当事者が事業契約を実際に締結するかどうかが依然として不確実な場合にも行われる。そのような状況では、評価、市場分析、将来のプロジェクト予測のために当事者間で情報を共有する。また、交渉段階で取引が決裂した場合、NDA が締結されていれば、両当事者は、共有したデータが自社に不利になる形で使われることはなく、また第三者に譲渡されることもないと確信できる。

(iii)NDA はまた、資金調達を望む企業と見込み投資家との議論に先立ち締結すべきである。このような場合、NDA は、競合他社が自社の営業秘密や事業計画を入手することを防止するためにある。

(2)　契約

契約は、一種の二者間合意であり、あらゆる一般的な状況下において利用可能である。NDA／守秘義務契約は、特定のタイプの合意又は契約であり、署名者は、営業秘密又は機密情報を第三者に開示しないことを約す。この NDA への違反があった場合、署名者に法的責任を負わせることができる。NDA は、通常、雇用の際や出資企業との間で合弁事業を立ち上げる際に交わされる。 一方、一般的な契約は会社合併等の際に締結される。役務提供契約の中で機密情報及び営業秘密に関する従業員及びコンサルタントの職務を規定し、その職務の内容及び対象となる情報の内容を明確化することは有用である。契約上の義務は、コモン・ロー又は営業秘密関連規制に基づく請求に比べ、通常、履行強制しやすい。

情報を機密／秘密に保持するための契約は、雇用主と従業員及びライセンサーとライセンシーとの間、並びに当事者間で秘密／機密情報が共有される場合のその他すべての当事者間で締結されるべきものである。契約書中には、当該契約に明記された目的以外の目的のために当該契約に基づいて入手した情報を漏洩又は使用しないという、negative covenants を課す制限条項を設けるべきである。1872 年インド契約法第 27 条は、このような規定に特に言及したものだ。

(3)　従業員との秘密保持契約

営業秘密が従業員によって不正利用されないことをより徹底するために、営業秘密の保有者は、秘密保持契約を結ぶべきである。企業によっては、当該企業に関する機密情報にアクセスできる従業員に対し、入社時の NDA 締結を義務付けている。従業員による窃取から営業秘密を守るには、新入社員の入社時に NDA を締結するだけでは不十分である。情報を営業秘密として保持する（従業員向けの）取り組みとして、以下の措置を講じるべきである。また、従業員／情報利用者が在宅勤務を行う場合や、営業秘密を守るための管理体制を構築する場合にも、これらの措置は有用となる。

・当該情報に「機密」との表示を付し、会社の機密情報を扱っていることを従業員が認識できるようにする。
・アクセス承認を受け、NDA を締結するまで、営業秘密又は機密情報へのアクセスを許可しない。
・パスワード保護、暗号化、及びファイアウォールの要件を含む、在宅勤務者向けの方針と手順を策定運用する。

・公共の Wi-Fi ホットスポットやその他のセキュリティが確立されていないロケーションから会社のネットワークにアクセスする場合、リモートで業務を遂行するすべての従業員にセキュアな VPN の使用を義務付ける。
・データプライバシー＆ガバナンスフレームワークを導入し、従業員に対し機密データへのアクセスを制限する。 ガバナンスフレームワークは、上級管理者及び運用レベルの管理者が、データの機密性を維持するための明確な基準と実践を確立するためのメカニズムである。データプライバシーは、従業員や顧客の財務データ、知的財産、個人の健康情報などのデータを適切に処理するためのものである。
・データ損失防止（DLP）ツールなどのソフトウェアツールを使用して、機密データを監視及び保護する。
・会社の営業秘密を守ることの重要性及びフィッシング攻撃の識別法について従業員教育を行う。
・重要な資産を特定し、多層防御の原則に基づき何層にもわたるセキュリティを実装する。
・極めて機密性の高い情報については、認証を受けていないユーザーが認識された場合、又は携帯電話のカメラを用いた画面撮影をソフトウェアが検知した場合にコンピュータをロックする顔認識ソフトウェアを活用する。
・従業員の PC からのすべてのインターネットトラフィックを会社のファイアウォール経由で監視し、異常なトラフィックとサイトへのアクセスを監視する。

(ii)データベースの保護　営業秘密を格納するデータベース、サーバー、及びソフトウェアへのアクセス権を持つユーザーを制限する。サーバーをパスワードで保護すると共に機密情報を入力する際にコンピュータ画面に適切な警告が表示されるようにし、機密の文書、フォルダ、スクリーンセーバーはパスワードで保護し、ファイアウォールのような電子的セキュリティチェック、アンチウイルスその他あらゆる種類の保護ツールを活用して、コンピュータファイルの写しの形をとった機密情報が会社の業務に影響を与える社外に漏洩しないよう、確実な対策を講じる。

(i)退社時の諸確認　従業員が退職する前に退職時の諸確認をスケジューリングすることが重要となる。会社の営業秘密を保護するため、当該従業員には、道義的及び法的責任を告知し、再認識させるようにする。当該従業員が守秘義務契約締結済みかどうかを確認させるようにする。また、引き続き守秘義務があることを確認する文書に署名するよう従業員に求めることも効果的な措置となり得る。会社に関するすべてのメモ、書類、文書を返却するよう従業員に求めるようにする。

(4) 産業スパイからの営業秘密の保護

産業スパイから営業秘密を保護し、その手に渡ることを防止するために取るべき措置は以下の通り。

(i)会社が所有する秘密情報の特定

自社が保有している営業秘密がどのようなものであるかを正確に把握することは、営業秘密を守るための第一歩である。そのためには、社内・社外のいずれについても検討することが必要となる。自社の営業秘密の真の価値を把握するため、企業は、競合他社の技術や業界のベストプラクティスと比較して自社の営業秘密がどのレベルにあるかを理解する必要がある。自社の知的財産を適切に評価することで、自社にとって最重要な秘密をより良く守るため、より効果的に優先順位を設定し、セキュリティ資源を投じることができるようになる。

(ii)脅威の特定

産業スパイを防止する戦術の策定に先立ち、企業は、最も脅威となるグループを特定しなければならない。たとえば、誰の目から見ても明らかな脅威となり得るのは自社の競合企業である。

(iii)物理的セキュリティ

企業は、インフラ、ツール、オフィスが物理的に確実に保護されるよう図らなければならない。これには、監視装置の設置、エントリーポイントの保護、セキュリティ専門家の臨時又は恒久的な雇用が含まれる。企業は、最も機密性の高い施設及びデータの特定・保護に特に注意を払わなければならない。

(iv)バックグラウンドチェックの実施

企業は、機密情報にアクセスできるすべての従業員のバックグラウンドチェックを実施しなければならない。また、企業は、初期スクリーニング後も、定期的に従業員に対するセキュリティ評価を行うようにする。

(v)サイバーセキュリティの確保

近年産業スパイ活動にコンピュータネットワークが利用されるケースが増加している。そのため、企業にとって、強力なサイバーセキュリティシステムを維持することは重要である。データベースは、強力なパスワードを使用して保護しなければならない。

(5) 適切な秘密保持契約を締結するには

NDAすなわち「秘密保持契約」とは、各当事者が秘密に保持しなければならない情報とはどの情報かを明らかにする、複数当事者間の法的契約である。NDAは、企業により、従業員、見込取引先等が当該企業の機密情報を漏洩しようとした際に自社を守れることができるよう用いられる。NDAは、企業の営業秘密その他の情報が一般公開されたり、競合他社に漏洩することを防ぐ上で有用である。

漏れのない優れた NDA となるようにするため、契約書中に以下の要素が含まれるようにしなければならない。

(i)　NDA の対象となる全当事者の特定

NDA は、当該企業と秘密情報が委ねられる者を冒頭部分に明記する。NDA は、可能な限り具体的に、契約書中に含むべきすべての当事者及びサブパーティー、並びに当該企業の営業秘密を秘密に保持することが求められるその他の者、例えば、当事者のうち 1 者からの購入者又はいかなる形式であっても関与する者のような契約や取引の当事者ではないが関与する者又は組織の名称を記載する。

(ii)　明確に定義された機密情報の成立要件

曖昧さを排し、他方の当事者が機密情報の範囲を認識できるよう、NDA には機密情報の正確な定義を記載するよう図る。

(iii)　情報受領者の責任

このセクションでは、情報受領者が入手することとなる企業秘密に対し、当該情報受領者は何ができ、何ができないかを記載する必要がある。

(iv) 契約に係る期間の決定

契約に係る期間にかかわらず、特許又は著作権により保護されている情報については、当該情報を開示した企業が完全な所有権を保持し、NDA の満了後も当該情報を濫用した場合は法的措置の対象となる可能性があるとの条項を含めることが望ましい。

(v)　秘密保持契約からの除外項目

この合意を関係者全員にとって網羅的かつ正当なものとするため、NDA の対象とならない情報の種類を明記することは有用である。大多数の企業にとっての標準的な除外項目として、既に公知である情報、情報受領者が既に第三者から知らされている情報、法律により開示が義務付けられている情報などがある。

企業に対する法的保護と、相手方がその条件を受け入れられる程度の許容性とのバランスが取れたものが理想的な NDA と言える。NDA の究極的な目標とは、裁判で争うような状況を作らないことにある。

第 3 章　営業秘密漏洩時の対応

例えば

- ・情報漏洩の兆候
- ・初動対応（紛争解決手続及びロードマップ）
- ・民事上の解決法
- ・刑事上の解決法
- ・その他の紛争解決法（行政上及び／又は多国間の措置、ADR 等）

(1)　情報漏洩の兆候

ほとんどの場合、営業秘密又は機密情報は、従業員によってうっかり又は誤って漏洩される。これは、雑談、就職面接、又は同様の状況で起こり得る。

また、業務のデジタル化への急速な移行により、保管されているデータや在宅勤務者のデータへのアクセスに対する保有者／会社のコントロールがより脆弱になり、データ盗難その他の機密保護違反のリスクが増大している。

さらに、従業員や元従業員が会社に損害を与えたり、報復したりしようとするケースもあり、そのような場合、悪意を持った意図的な情報漏洩が往々にして起こる。

この他、競合他社の活動を監視することは、営業秘密の漏洩把握のための重要な取り組みである。同様に、競合他社が発売した製品が自社製品と酷似している場合や、競合他社が自社従業員と頻繁に面談している場合についても、営業秘密漏洩の可能性がある。

(2)　初動対応（紛争解決手続及びロードマップ）

営業秘密の保有者は、当該企業の機密情報が漏洩していることを知った場合、必要な措置を速やかに講じるべきであり、また、漏洩者に対する刑事上又は民事上の措置についても検討する必要がある。機密データが盗まれた場合、当該データの保有者は、事態を調査し、損害を判断するための措置を直ちに講じるべきである。また、サイバー犯罪調査の専門家は、データが盗み出されたシステムについての調査分析を支援することができる。

契約又は秘密保持契約に対する違反及び営業秘密の不正利用に対しては、金銭的損害賠償の支払いを求め提訴することが可能である。多くの場合、立証責任は原告側にあり、機密情報又は営業秘密として保護しようとする情報を明らかにしなければならない。

一度営業秘密が漏洩してしまうと、秘密が保持された状態の回復はほとんど不可能

である。それ故に、営業秘密を保護するため、適切な措置が取られなければならない。インドには、営業秘密の保護に関する厳格な法律は存在していないものの、上の各項で解説したように、裁判所は、公正、正義、良心という概念に基づき、営業秘密保護に関連した訴訟の判決を下している。

営業秘密の不正利用は、不正な手段による営業秘密の開示であると理解されているが、これに対する特別な法は存在しない。したがって、営業秘密の不正利用又は不正開示に対する訴訟が起こされる場合、一般的にその訴因とされるのは、民事訴訟では契約違反及び不正利用による不正行為、刑事訴訟では窃盗及び背任などである。

民事訴訟においては、差止命令及び損害賠償とは別に、原告又は権利者が行使することができるその他の民事上の救済措置には、営業秘密を含む資料（例：紙資料やUSB等の情報を記録した記録媒体、金型等の情報を化体した物件）の返還又は営業秘密を含む資料の返却を認める裁判所命令、及び被告により悪用された資料を（損害賠償額算定のために）保管するための裁判所委員の任命などがある。裁判所は、裁判所委員が裁判所による適切な捜索・差押命令を遂行するに当たり、地域の警察に対しこれを補佐するよう指示することもできる。

刑事訴訟においては、1860 年インド刑法及び 1957 年著作権法（著作権を保護）や 2000 年情報技術法（電磁的記録を規律）など特定のテーマに関する法律に、禁錮刑又は罰金刑に処せられる可能性のある犯罪を具体的に規定する条項が含まれている。営業秘密の不正利用を犯罪として具体的に挙げている例はない。ただし、事案の事実において、背任罪、窃盗罪、詐欺罪等の罪が適用される場合がある。背任罪に対する刑罰とは、３年以下の禁錮又は罰金である。委託を受けた財産を不正に流用し、又は自己の使用のために換金し、又は（明示的か黙示的かを問わず）契約又は適用される法令に違反して不正に使用又は処分し、又はその他の者にこれを許した場合、その者は背任罪を犯したものと見なされる。

さらに、NDA の中では、当該 NDA 中の条項の第三者による違反に対する損害賠償請求規定等大きな制裁も明記すべきである。営業秘密に起因する紛争について、インドにはそれに特化した裁判外紛争解決手続（ADR）は存在しないが、紛争が発生した場合に、調停（拘束力の有無にかかわらず）や仲裁を含む既存の ADR により裁判所外で紛争を解決できるよう、NDA には ADR 条項を含めて、それにより解決に向けた時間を節約できるようにすべきである。

第 4 章　各種事例、参考例

関連文書及びセルフチェックシート参考例、就業規則における守秘義務規定の例、従業員との秘密保持契約の例退職後の競業避止契約の例、取引先との秘密保持契約、取引先管理体制チェックシート来客、受付票（秘密保持契約）等セルフチェックシート（営業秘密保護方針の管理、営業秘密取扱管理、従業員管理、物的管理、通信セキュリティ管理等)。

職場の従業員又は取引関係にあるベンダー／パートナー企業との間で知的財産に関する契約又は方針を締結することが重要である。インドの中規模企業・団体は、その重要性を認識しており、一般的に、技術を開示する前に、NDA を締結している。同様に、知的財産権の譲渡に関する条項が、従業員向けの雇用契約中にも盛り込まれる。職場向けの営業秘密保持契約／方針により、対象事項の機密性や機密情報の性質、及び守秘義務に違反した場合、どのような結果を招き得るかについて、従業員及びスタッフに認識させることができる。

インドにおいて、契約書は履行強制可能なものとされているため、雇用／秘密保持に関する合意書又は契約は、営業秘密のような機密情報の保護に有用である。契約書は、機密情報の不正な開示及び不正利用を禁止する条項を含むよう作成すべきである。これらの契約書中には、開示される可能性のある情報の種類、そういった情報を用いる場合の注意、及び契約期間終了後の開示に対する制限も含めるようにする。

添付の就業規則における秘密保持関連条項のサンプルを参照のこと。機密情報の保護／従業員による機密情報の悪用に関し、一般的に、次のような条項が雇用契約に盛り込まれる。明確にしておくと、ベンダーとは、商品やサービスの購入と流通を扱う会社/個人を含む広い意味の文言である。　一方、メーカーとは、工具、化学薬品、機械などの製品の製造に携わる会社/個人である。

(1) サンプル１（従業員向け）

秘密保持及び知的財産権

(i)　あなたは、当社に雇用されていることにより個人的に知り得た技術的ノウハウ、オフィス管理、セキュリティ、ベンダーの詳細情報、メーカーの詳細情報、購入者の詳細情報、当社に関する事務及び／又は組織関連の事項に関する資料、細部又は詳細すべてについて、いかなる相手に対しても口頭又は書面で提供しないものとする。

(ii)　雇用期間中に［従業員氏名］が作成した商標／ブランド及び著作権を含むすべての知的財産権は、当社が独占的に所有する専有資産である。

会社の知的財産権の不正利用は、解雇につながる。

(2)サンプル２（従業員向け）

秘密保持

従業員は、本契約の過程において又は本契約に関連して、両当事者が［YY/MM/DD♠］に署名した秘密保持契約に従い、雇用主から受領したすべての情報を、機密として取り扱うことを約す。当該秘密保持契約の写しは、付属書［YY/MM/DD♠］として本契約に含まれる。本契約と秘密保持契約との間に矛盾が生じた場合、対応する秘密保持契約の条項が優先するものとする。

(3)サンプル３（ビジネスチャネル向け）

ベンダーとの契約書

添付のベンダー契約書サンプルを参照のこと。ベンダーとの契約書では、知的財産を特定すると共に知的財産に関する規則を明記するものとする。以下に例を示す

知的財産権

(i) 販売者は、購入者が、ブランド、ロゴ、タグライン、商標、特許、サービスマーク、営業秘密、著作権及び意匠、又は本契約に明示的に記載されていないその他の知的財産権（IP）を含む購入者の IP の専有的な保有者であることを確認し、これに同意する。購入者は、購入者の IP が第三者の IP を侵害しておらず、又は、第三者の IP に違反していないことを表明し、保証する。

(ii) 本契約の条件に基づき、購入者は、本契約が有効である間、商品製造用に購入者の IP を使用するための限定的、譲渡不能、非独占的なライセンスを販売者に付与する。

(iii) 販売者は、購入者の IP に酷似した、又は混同を招くおそれのある、購入者の IP に似た商標、サービスマーク又はトレード・ドレスを登録してはならない。

(iv) 購入者が付与した限定的なライセンスが存在する場合、当該ライセンスは本契約の終了時に満了する。

(v) 製品を製造するための下請先との契約／ライセンスを行う場合は、購入者の書面による正当な許可を得なければならず、当該下請契約は、購入者によるいかなる IP 権の独占的所有を維持するため、本契約に定めるのと同じ条件に従うものとする。

秘密保持

（i） 販売者は、商品の技術仕様を含め、特定の非公開機密情報、営業秘密情報（総称して「専有情報」）を購入者から受領する場合があることを確認し、これに同意する。
（ii） 販売者は、専有情報が購入者にとって価値があること、及びすべてのメモ、仕様書、フォーミュラ、技術仕様、アルゴリズム、図面又はその他の関連情報が秘密に保持されなければならないことに同意する。
（iii） さらにまた、販売者は、当該情報を使用せず又は第三者に開示しないことに同意する。販売者は、購入者が共有したすべての専有情報を、共有されたままの形で購入者に返却する。また、販売者は、購入者のいかなる専有情報についても、一切それを複写してはならない。

従業員と事業関連情報を共有する場合の営業秘密

従業員に共有される事業関連情報は、義務の履行強制にとって複雑かつ主観的なテーマとなる。これは、雇用期間中、従業員は担当する顧客やクライアントの身元を外部機器の助けを借りることなく記憶する可能性が高く、そのため、インド憲法第 19 条第 1 項（g）の下での取引及び職業の自由という基本的権利に基づき、従業員が当該情報を自由に使用できるためである。

退職後の競業避止契約の例

退職後の競業避止契約に関する情報はない。しかし、契約期間中は、制限的合意事項により雇用主の合法的な雇用に従事する現従業員は制約を受けるとの法的見解は確立されている。一方、契約終了後の従業員に対するこのような制限の有効性に関する法的見解は議論の分かれるところであり、複数の裁判所において判断が示されている。インドの裁判所は、複数の訴訟事案において、雇用期間中のネガティブコベナンツの履行強制は当事者間で可能であるが、雇用期間を超えて強制することはできないと明確化している。

雇用終了後の競業避止条項（制限条項とも呼ばれる）は、雇用終了後、雇用主の事業を保護するために、特定の期間又は特定の地域内で従業員が類似の事業又は職業に従事することを禁止することを企図し、契約に盛り込まれる。

インド憲法及び 1872 年インド契約法（以下「契約法」）の規定に照らし、一般的に裁判所は、雇用主と従業員との間の既存契約にかかわらず、従業員の生計に対する権利が雇用主の利益に優先されなければならないとの判断を示してきた。

インド憲法第 19 条（g）は、すべての市民に、あらゆる職業、取引又は事業を営む権利があることを明確に規定している。これは絶対的な権利ではなく、公益のために、この権利に合理的な制限を課すことは可能である。裁判所は、このような制限を認めることに対しては常に慎重であり、それぞれの事案の事実と状況に応じ、正義、道徳、公正の原則が適切に適用されるよう、この規定の解釈を柔軟に保ってきた。

第 27 条の条文からは、どのような制限が有効とされるかについて、窺い知ることはできない。インド最高裁判所は、1967 年 1 月 17 日の Niranjan Shankar Golikari 対 Century Spg & Mfg Co. Ltd 訴訟判決（1967 AIR 1098, 1967 SCR (2) 378）において、契約法第 27 条に基づく「制限的」契約の有効性を決定するための判断の拠り所として、以下のように詳述した。

「・・・契約終了後の期間中に制限を適用する場合と、契約期間中に運用する場合とでは、制限条項に対する見解は異なったものとなる。従業員が雇用主のみのために働く義務を負う雇用契約期間中に適用されるネガティブコベナンツは、一般的に取引の制限とは見なされず、したがって、契約法第 27 条に該当しない。従業員が雇用主の事業と類似した、又は実質的に似た取引もしくは事業に従事せず、又は他の雇用主のためにそのような職務に従事しないというネガティブコベナンツは、当該の契約が非良識的、過度に過酷、不合理、又は一方的でない限り、取引の制限とはならない」

以上の見解に照らし、当該契約は有効であり、それにより、上告人は、当該契約の期間中、他のいかなる企業に勤務することも禁止されるとの判断が示された。最高裁判所は、雇用契約には、元従業員が以前の雇用主の営業秘密を利用することはできないとの黙示の条件が存在するとの判断を示した。

デリー高等裁判所は、2015 年 1 月 22 日の Affle Holdings Pte Limited 対 Saurabh Singh 訴訟判決（OMP 1257／2014）において、契約期間後に競合事業を営むことを禁止する雇用契約中のネガティブコベナンツは無効であり、履行強制はできないとの判断を示した。この禁止は、契約法第 27 条の規定に基づいて適用されたものだ。

2013 年 1 月 20 日の LE India Tours 及び Travels Pvt. Ltd 対 Deepak Bhatnagar 訴訟判決（IA Nos. 15636／2013, 16770／2013 & 16817／2013 in CS (OS) 1881／2013）において、デリー高等裁判所は、雇用期間後に雇用されることを制限する雇用契約は、契約法第 27 条に基づき保護されないとの判断を示した。

2006 年 7 月 11 日の Wipro Ltd. 対 Beckman Coulter International SA 訴訟判決（2006 (3) ARBLR 118 Delhi, 2006 (2) CTLJ 57 Del, 131 (2006) DLT 681）において、

裁判所は、雇用主と従業員間の契約について、より厳しい見方を示した。これは、取引において両当事者が多少の程度の差はあれ対等な立場でいるべきことが期待されることによるものだ。通常、このような契約では、雇用主が従業員よりも有利であり、従業員が標準書式の契約書に署名するか、さもなければ雇用されないかを迫られるケースが極めて多い。

雇用契約終了後／退職後の競業避止義務条項については、インドの司法制度においては、明確なスタンスがない。雇用契約終了後の競業避止条項を履行強制できるかどうかについての司法判断は、雇用主の利益保護のために設けられたものであっても営業秘密及び秘密保持契約の非開示などのネガティブコベナンツが必ずしも取引を制限するものではないことを暗に示している。しかし、インドの裁判所は、従業員に契約内容を一語一句違えず履行させる結果となるような場合、個人の役務提供契約に盛り込まれたネガティブコベナンツに対する違反行為を禁止する差止命令を発したことはない。制限的条項の有効性は、当該制限の期間と地理的範囲を含む合理性の基準によりその当否が判断される。

企業は、営業秘密／機密情報を保護する方針を維持し、定期的に方針を見直し、スタッフ／従業員に営業秘密及び会社にとってのその重要性について教育しなければならない。

来客受付票

訪問者に対しては、機密情報を保護するため、以下を実践することが推奨される。

(i) 自社事業のための来客者についての方針を策定する。

(ii) 事業拠点への来客について登録を行うようにする。

(iii) 不注意により制限区域に入ることのないよう、訪問者には必ず同行者を付ける。

(iv) 自社の営業秘密、ノウハウ、又は機密情報を目にする、又は推察される可能性のある制限区域を来客が訪問予定の場合、訪問前に秘密保持契約に署名してもらう。

(3 セルフチェックシート

企業は、営業秘密を保護するための一般的なプロセス及び文書を活用することができる。チェックリストの内容について、インターネット上から情報を収集した。チェックリストの例を以下に示す

例１

営業秘密とは何かを決定する

□ 営業秘密情報を特定する
□ 具体的に
□カテゴリー別に
□営業秘密情報の所在場所を特定する
□営業秘密情報にアクセスできる者を特定する
□当該情報は社内のみでアクセス可能か
□当該情報に第三者がアクセスすることは可能か
□当該情報は、事業でどのように活用されているか
□営業秘密を具体的に特定し、当該営業秘密の所在場所及び当該情報にアクセス可能な者を特定した文書を作成する

手順と方針 -- 社内
□営業秘密情報へのアクセスを制限する
□定期的な監査を実施し、コンプライアンスのモニタリングと評価を行う
□営業秘密情報を含む文書には「機密」というマーク／スタンプを付す
□どのような情報が営業秘密と見なされるかについて従業員を教育する
□営業秘密情報を含む文書についての文書取扱手順を策定する
□営業秘密情報を含む文書へのアクセスを制限する一知る必要のある者のみにアクセスを認める
□営業秘密情報を含む文書にアクセスするためのサインイン／サインアウト手順を策定する
□営業秘密情報を含む文書は、自社敷地又は自社敷地内の一定の区域から持ち出せないようにする
□方針及び方針遵守確認のためのモニタリング状況について定期的にアップデートを行う
□営業秘密情報を含む文書は、他の業務関連文書とは区別して保管する
□営業秘密情報を含む文書の文書取扱手順に関し、従業員を教育する
□営業秘密情報を含む文書の自社敷地からの持ち出しに関する手順を策定実施する
□営業秘密及び機密情報を含む文書の複製は数を限る
□主要な従業員及び営業秘密情報へのアクセス権を有する従業員との間で、独立した秘密保持契約を締結する
□営業秘密と見なされる情報は、個別に営業秘密情報として特定する
□営業秘密情報を含む文書の追跡及び破棄に関する手順を策定実行する
□全社的な秘密保持方針を定め、全従業員に対し、当該方針を理解したとの署名を義務付ける

□従業員ハンドブックには、従業員のプライバシーは期待されていない旨の記載をするようにする
□従業員及びフリーランスの請負業者との間で職務著作物／職務開発物契約を締結する
□文書保管方針を策定する
□電子メール方針を策定する
□全従業員に対し方針についての最新情報を提供する
□すべてのコンピュータ、ノート PC、タブレット、スマートフォンは、会社所有のものを使用させる
□重要な文書及びソフトウェアを保護するため、著作権を取得する
□発明、ビジネスプロセス及びソフトウェアを保護するため、特許を取得する
□方針と手順の遵守状況をモニタリングし、遵守状況をモニタリングするための取り組みについて周知する

手順と方針　従業員の退職時
□期間満了となった及び退職した従業員のアカウント及びネットワークアクセス権を無効にする
□退職前に、従業員のノート PC その他のデバイスの確認及び／又はコピーを実施する
□全従業員に対し退職時面談を実施する
□新たな雇用主に関する情報を尋ねる
□新たな肩書及び責任に関する情報を尋ねる
□退職する従業員に、新たな雇用主に対して秘密保持契約及び秘密保持義務の存在を通知する必要があることを再確認させる
□従業員に秘密保持義務があることを再確認させる
□従業員に秘密保持契約書の写しを提供する
□会社書類その他の会社財産を返還させる
□従業員に秘密保持義務の存在及び会社書類及び会社財産を返却すべきことを理解したと書面により提出させる
□退社時面談を記録として残す

物理的なセキュリティ対策
□必要に応じ、従業員に身分証明書又は身分証明カードの提示を求める
□必要に応じ、来客管理の仕組み（ビジターバッジ等）を構築する
機密情報を含む引出しや区域は分離・施錠する
□従業員の私物であるデバイス上での会社情報の使用に関する方針を策定実施する

□コンピュータセキュリティ対策を実施する
□異なるアクセスレベルごとのパスワード保護を実施する
□定期的にパスワード変更を要求する
□複数の文字種を組み合わせたパスワードを要求する
□データベース／ファイルに制限をかける
□ノート PC にセキュリティ対策を施す
□営業秘密データは暗号化する
□ポータブルストレージデバイスの使用状況を監視する
□コンピュータから外部ポートを取り除く
□インターネットアクセスを管理する
□退職した従業員のコンピュータに関し、問題の有無を確認する
□退職した従業員のハードディスクをコピーする
□コンピュータ監視用機器を導入する／コンピュータ利用を監視する
□営業秘密情報は暗号化する
□ウイルス及びマルウェアに対する適切な保護を実装する
□廃棄するコンピュータ機器はすべて、廃棄前に必ずデータ消去を行う
□営業秘密情報を含む文書はシュレッダーにかける
□営業秘密プロセスの不正な閲覧を防止するため、物理的障壁を設置する
□「立入禁止」及び／又は「立入禁止区域」の標識を掲示する
□物理的セキュリティ対策総合計画を策定する
□囲いを設置する
□出入人数を制限する
□アラームを利用する
□セルフロックドアを利用する
□時間外セキュリティ装置を利用する
□セキュリティ対策が施されたゴミ箱を利用する

手順と方針ー社外
□第三者に提供する営業秘密情報の提供方針を策定する
□営業秘密情報を入手するための条件として、第三者に秘密保持契約の締結を義務付ける
□営業秘密と見なされる情報は、個別に営業秘密情報として特定する
□第三者との契約に守秘義務／秘密保持規定を盛り込む
□第三者に提供した営業秘密情報を追跡するための方針を策定する
□営業秘密情報を保護するために第三者が講じた措置を定期的に監査する

その他の対策

(i) 外部開示審査の仕組み

機密情報が、マーケティングその他の公開資料（ホワイトペーパーやウェブサイト等）に掲載されないよう図る

(ii) 不注意による開示

開示された情報の拡散を制限し、不注意のせいで開示が行われた相手からの資料の返還を求める仕組みを含む、機密情報が不注意のために開示された際の迅速な対応策を策定する

(iii) 監査

営業秘密監査を定期的に実施し、方針が引き続き遵守されていることを確認し、文書化する

例２

2. 営業秘密の保護ーセキュリティ対策

☐ 機密資料には「機密」マークを付ける

☐ 物理的又は電子的に機密情報へのアクセスを監視、分離及び制限する

☐ 機密情報へのすべてのアクセスを記録する

☐ 自社敷地からの情報の持ち出しを禁止する厳格な制限／ルールを設ける

☐ 機密情報を閲覧できる可能性のある場所へのアクセスを制限し、そのような場所への記録装置の持ち込みを禁止する

☐ 第三者との間で確実に秘密保持／守秘義務契約を締結する

☐ 自社敷地外での自社技術の使用手順を策定する

☐ 電子的に保存された情報をパスワードで保護する

☐ 適切なファイアウォール、ウイルス及びマルウェア対策のためのメカニズム、暗号化その他のハッカー対策を講じる

☐ 訪問者に対し、機密情報を保管していた場所で閲覧／アクセスした情報を開示することを禁止する

3. 営業秘密の保護ー従業員管理

研修及び秘密保持方針

☐ 秘密保持方針を策定・配付して、従業員に対し、営業秘密を守るという自らの義務を再認識させる

☐ 秘密保持方針を受領すると共に研修を受け、その内容を理解したとの書面による確認を従業員から取得する

☐ 秘密保持の重要性について、従業員教育を行う。秘密に保持すべき情報を定義する

従業員契約

☐ 営業秘密に関連する従業員は、秘密保持、守秘義務、所有権及び競業避止に関する条項を含む契約に署名するものとする

従業員の退社手続

☐ すべての従業員契約の写しを提供する

☐ 従業員に秘密保持に対する義務を再認識させる

☐ 新たな雇用主が競合企業かどうかを判断するため、退職時面談を実施する

☐ 会社に対する物理的／電子的アクセスのいずれについても遮断する（パスワードの変更、鍵等のアクセスの仕組みの返却等）

☐ 営業秘密の窃盗リスクを評価するため、通信記録（コンピュータ、ハードドライブ、電子メール等）を確認する

☐ 退職する従業員は、会社関連の資料をすべて返却しなければならない

(1) 採用内定通知書

日付 _____

氏名
住所１
住所２

_____様（以下「従業員」という）

貴殿のご応募及びその後の当社での面接につきまして、以下の条件のとおり、当社での_____の職での採用の内定を通知いたします。

報酬

基本給	_____
住宅手当	_____
通勤手当	_____
個人旅行手当	_____
医療手当	_____
特別手当（もしあれば）	_____
賞与	業績連動・自由裁量

本契約期間中、従業員の給与は、銀行送金、小切手、又は雇用主にとって都合のよいその他の方法で支払われるものとし、従業員はこれに同意するものとする。

上記に加えて、貴殿の希望は、法律に従い、現行の会社方針によって取り扱われる。

試用期間

1. 入社日から３ヵ月間は試用期間とする。試用期間は、人事部が求める書類を貴殿が提出した時点で開始する。当社は、貴殿の勤務成績が満足できるものでないと認められる場合に、本契約を終了し、又は試用期間を当社が必要と判断する期間延長する権利を有する。

2. 試用期間中、いずれの当事者も、相手方当事者に２週間前の通知を付与するか、又は通知に代えて支払いを行い、本労働契約を終了することができる。貴殿の試用期間の終了を当社が確認した後は、終了通知期間は、２ヵ月前に変更されるか、もしくはその代わりに支払うか、又は相互に合意したそれよりも早期の期間に変更される。

年次昇給

1. 給与は、年１回、_____月又は_____月_____日に見直される。昇給の査定は、貴殿が当社での１年間の在職期間を満了した後にのみ適用され、専ら経営者の裁量により決定する。当該査定においては、貴殿の勤務成績及び業務上の行動が考慮される。
2. 昇給査定時の在職期間が９ヵ月以下の場合は、当社の人事方針に従い、評価・昇給の標準的な評定基準が適用され、賞与の支給対象外となる。業績評価時の在職期間が９～12 ヵ月の場合、当社経営陣の裁量により、賞与は日割計算により支給される。
3. 給与のその他の調整は、当社の単独の裁量により行われる。
4. 当該雇用又は税体系の変更に起因するすべての納税義務は、貴殿が負担するものとする。

勤務時間

1. 当社の通常の就業時間は月曜日から金曜日の午前 10 時から午後６時までとする。
2. 当社は、必要に応じて、週末及び休日又はそのいずれかにおいて、不規則な勤務、超過勤務又は出張を要求する権利を有する。
3. 当社は、その業務要件を満たすように勤務時間を随時変更する権利を有する。

勤務地・異動

勤務地は、. . . . . にある当社の本店所在地とする。当社は、事業上の要件に基づき、従業員を自己の支店、子会社又は関連会社のいずれかに異動／転任させる権利を有する。

休暇取得の権利

1. 現行の会社方針に従い、１暦年につき 29 日の休暇が与えられる。内訳は以下のとおりとする。

- 臨時休暇－７日間（未消化の場合は失効）
- 医療休暇－７日間（未使用の場合は失効）
- 特別休暇－15 日間（最大３年繰り越すことができるが、45 日の休暇を上限とする）

出産・育児休暇－女性従業員は、第１子の場合、26 週間の出産・育児休暇を取得することができる。第２子以上の場合は、12 週間の出産・育児休暇を取得することができる。男性従業員は、15 日間の出産・育児休暇を取得することができる。この休暇は、出産日の 15 日前から、又は出産日から６ヵ月以内に取得することができる。

2. 祝日は追加され、各暦年の初めに祝日一覧が貴殿に配布される。

3. 臨時休暇及び特別休暇を取得する場合は必ず、直属の上司の事前承認を得なければならない。

4. 別段の指定がある場合を除き、正午以降に職場に到着した場合は、半日休暇が差し引かれる。

5. 貴殿が傷病により連続して３日を超えて欠勤する場合、雇用主に対し自己申告書式を提出しなければならない。当該欠勤が連続して７日を超える場合、医師の診断書を取得し、雇用主に提出しなければならない。

秘密保持及び知的財産

1. 貴殿は、いかなる者に対しても、当社との雇用関係により個人的に知り得た、技術的ノウハウ、会社経営、安全対策、販売業社の詳細、製造業者の詳細、購入者の

詳細、当社に関連する事務的及び組織的又はそのいずれかに関する事項の、資料、明細又は詳細を、口頭又は書面を問わず、提供しないものとする。

2. 職務上貴殿が創出した著作権を含むすべての商標／ブランド及び知的財産権は、当社が単独で排他的に専有する財産である。当社の知的財産権を濫用することは、雇用終了の原因となる。

職務の遂行

1. 雇用期間中、以下について合意する。貴殿は、当社の業務に全就業時間を費やし、誠実かつ効率的に貴殿に割り当てられた義務を遂行し、かつ貴殿の能力の最大限の発揮により、目標を達成し、当社が設定したパラメーターを遵守するよう努力するものとする。

従業員の一般的義務

1. 当社は、貴殿が最大限の公正さ、誠実さをもって勤務し、当社が策定又は実践する**ビジネス基準及び関連する規範**に従うことを期待する。

2. 貴殿は、貴殿の雇用期間中、適用される**規則及び規定**（随時施行、修正又は変更される）に従うものとする。

3. 貴殿は、その都度、経営者の事前の書面による許可を得た場合を除き、報酬を得るために、直接又は間接の業務を引き受けず、又は名誉職の仕事を行わないものとする。

4. セクシュアル・ハラスメントを行うことは禁止されており、また、就業施設の内外を問わず、就業中にいかなる形態のセクシュアル・ハラスメントも行わない。貴殿は、本契約の本条件に違反した場合、自身の行為につき全面的に責任を負うものとし、当社は、貴殿が行った違法行為につき一切責任を負わないものとし、貴殿の雇用は、払戻し又は退職金なしに、即時発効で終了するものとする。

5. 貴殿は、貴殿の雇用の有効期間中、及び貴殿の退職日から６ヵ月間は、競合する類似のいかなる事業にも従事しないものとする。

6. 貴殿の任命は、貴殿が業務に参加した日に発効する。

変更

本契約の変更又は本契約に関連していずれかの当事者が負う追加の義務は、それが書面により証明される場合に限り、拘束力を有するものとする。

修正及び終了

1. 当社は、貴殿に少なくとも１ヵ月前の事前通知を行うことにより、貴殿の雇用をいつでも終了させることができる。

2. 当社が雇用を終了する場合、当社は、終了の事前通知、又は１ヵ月に相当する事前通知に代わる補償を、貴殿に対し提供するものとする。

3. 貴殿は、当社に２ヵ月前の事前通知を行うか、又は当該通知に代えて相当額の給与を支払うことにより、貴殿の雇用を終了することができる。

本任命を承諾したことの証として、正式に署名された採用内定通知の複製物を返送してください。

当社の組織に貴殿が来られることを歓迎し、当社での貴殿の成功を祈念いたします。

経営者

承諾

私は、上記の条件に同意し、_____までに入社するものとします。

署名：
日付：
氏名：

(2)　知的財産に関する合意書

本知的財産に関する合意書（「本契約」）は、[・]（「締結日」）に、[・]で、以下の両当事者間で締結される。

1.　一方当事者として、……..

（以下、「**当社**」又は「**雇用主**」といい、この表現は、その文脈又は意味と矛盾しない限り、そのグループ会社、関連会社、承継人及び譲受人を意味し、かつこれらを含むとみなされるものとする）。

2.　他方当事者として、[·]（以下、「**本従業員**」又は「**発明者**」といい、この表現は、本契約の意味又は文脈と矛盾しない限り、その承継人及び許可された譲受人を含むものとする）。

以下、当社及び本従業員を総称して「**両当事者**」といい、個別には「**当事者**」と呼ぶ。

前文：

a)　本契約は、新たなイノベーションの創出及び知的財産保護の重要性を強調する。 当社は、顧客の産業のコアプロセスの生産性向上を図り、ひいては競争力を確保するための新たな取り組み方法を継続的に模索している。当社は、新規技術を生み出し、当社の特許、意匠保護、商標、著作権、ドメイン名、営業秘密、サービスマーク、データベース権、意匠権、著作者人格権又はその他の財産権（それぞれ、登録されているか否かを問わず、また登録出願がある場合はその出願を含む）で構成され

る（ただし、これらに限定されない）知的財産権に関する様々な法律により、これらの新規技術を保護することを目指している。

b) 本契約の文脈において、「**知的財産**」とは、商標、商号、サービスマーク、サービスマーク登録、サービス名、特許、特許権、著作権、発明、ライセンス、許諾、政府許可、概念及び開発、プロセス、製品、ソフトウェア及びそのプログラム、公式、アイデア、意匠、ソースコード、オブジェクトコード、アルゴリズム、営業秘密、製法、設計図、ノウハウ、ドメイン名、アプリケーション、データ、アイデア、技術、アイデア、文書、メモ、プレゼンテーション、著作物、ビジネスプラン、顧客リスト、ユーザー情報、ベンダーデータ、顧客データ、営業データ、及び本従業員が雇用期間中に作成、考案、開発、改良又は提供した実際の又は予想されるビジネス、研究又は開発に関するその他の情報を含むが、これらに限定されない情報を意味する。

c) それゆえ、本従業員は、当社との雇用期間中、及び本従業員が当社と締結する雇用契約に定める本従業員の義務の履行のために、当社の知的財産の開発を考案し、これに貢献することができる。

d) したがって、両当事者は、本契約を締結して、本従業員と共有される情報における、発明の管理プロセス、職務発明に関する統一された手順、及び知的財産権の帰属に関する条件を定めることを希望する。

当社が提供する雇用及び以下に記載されるその他の相互の約束及び合意（その受領及び十分性がここに確認される）を約因として、両当事者は、以下の条

件に拘束されることに合意する。

1. 定義

本契約において、文脈上他の意味に解すべき場合を除き、以下の原文表記時に大文字で始まる用語は、それぞれの文法上のバリエーション及び類似表現とともに、本契約に定義される意味を有するものとする。

関連会社とは、当事者に関して、直接又は間接を問わず当該当事者によって支配されている、直接又は間接を問わず当該当事者を支配している、又は直接又は間接を問わず当該当事者を支配している会社又は法人によって直接又は間接を問わず支配されている事業体を意味する。

「本契約」とは、本契約、付属文書、別表、別紙及び本契約の一部として特定されるその他の文書を意味し、当該契約及びその他の文書は随時修正又は変更される場合がある。

「付属文書」とは、本契約のすべての付属書、付属文書を意味する。

「秘密情報」とは、本契約の締結もしくは履行の結果、又は本契約に起因する紛争において本従業員が受領もしくは取得したあらゆる情報（本知的財産に関連する商業的又は技術的又は財務的情報を含む）を意味する:

本契約の条件

本契約に関する交渉

本契約の履行

本契約に基づき交換又は提供される、技術的その他を問わないすべての文書（計算、図面、マニュアル、モデル、コード及び本契約に従い雇用主が本従業員に提供又は開示する技術的性質又はノウハウの電子形式を含むその他の文書を含む）

雇用主又はその関連会社の事業、戦略又は見通し（モデル、市場調査、顧客名、報告書、予測、データ、ノウハウ、営業秘密、アイデア及び環境アセスメントの結果を含む）。これには、本従業員が入手可能な情報も含まれる。

「支配」とは、事業体に関して、以下のいずれかを意味する。

a. 被支配事業体の株式資本、議決権株式等の 50%以上の所有又は支配（直接的か否かを問わない)。
b. 被支配事業体の取締役会、経営委員会、又は他の同等もしくは類似の機関について、その支配権、その構成を支配する権限、又はその構成員の過半数を指名する権限を付与する、契約その他による株式資本、議決権株式等の所有。

「**発明**」とは、特許性があるか否かを問わず、また当社との雇用期間中に（単独であるか他者と共同であるかを問わず）実施化したか、又は発明者自身が作成もしくは考案したかを問わず、すべての発見、プロセス、設計、技術、装置、又は前述もしくはその他のアイデアの改良であって、当社の実際のもしくは明らかに予想される事業、業務又は研究開発に何らかの形で関連するもの、又は発明者に割り当てられた業務、もしくは当社のためにもしくは当社に代わって発明者が遂行する業務に起因するかもしくは示唆されるものを意味する。

「**著作物**」とは、文芸作品、芸術作品その他の著作物（製品の技術説明、ユーザーガイド、イラスト、宣伝資料、コンピュータプログラム／ソフトウェア及び当該資料への寄与分を含むがこれらに限定されない）を意味する。

「**対象発明**」とは、本従業員が考案し、かつ当社が本従業員を雇用したことにより間接的又は直接的に生じた発明を意味する。

「**対象著作物**」とは、本従業員が考案し、かつ当社が本従業員を雇用したことにより間接的又は直接的に生じた著作物を意味する。

「対象外発明」とは、雇用開始前に存在した、従業員の知的財産、又は雇用主のリソース、設備、備品、施設、秘密情報もしくは日程を使用することなく、完全に従業員自身の時間に基づいて開発された知的財産を意味する。

「宣言」とは、インド／条約国において出願人に対する発明者／本従業員による発明者の地位に関する宣言を意味し、特許出願の出願人が発明者／当社の譲受人又は法定代理人であることを宣言するものである。

締結日とは、本契約の締結日を意味する。

2. 職務発明に関する法令

a) 本従業員は、本契約が当社及びそのすべての関連会社及びグループ会社における発明に関連するものであることを了解し、これに同意する。本契約は、本従業員が自身の雇用中に行ったすべての発明を含む。雇用主が従事している事業において有用な、又はこれに関連する発見、改良、開発、ツール、機械、器具、装置、コンセプト、デザイン、コンピューター・ソフトウェア・プログラム、販売促進アイデア、生産プロセス又は技術、実践、製法、及び新製品を含む職務発明であって、特許性があるか、著作権保護が可能か、又はその他を問わず、雇用主が雇用中に本従業員が作成、発見、開発又は保証し、雇用主における本従業員の雇用の主題に関連するものは、インド契約法及びインド特許法に従い、本契約に準拠するものとする。

b) 本従業員は、必要に応じて、以下のことに同意する。__の知的財産権チームは、職務発明に関連する事項について、更なる指示を与えることができる。

3. 発明の記録の保持

a) 本従業員は、本従業員の当社での雇用に関連して本従業員が考案し、創作し、又は今後創作するすべての発明及び著作物を、速やかにかつ書面で当社に対し開示する。また、本従業員は、かかる発明又は著作物が適宜、対象発明又は対象著作物であるかどうかを決定することがで

きる形式で、かかる開示を行う。本従業員は、対象外発明に関連する場合を除き、自らが、単独又は他者と共同で、いかなる発明、特許登録もしくは出願、又は著作権登録もしくは申請も有しないことを当社に対し表明する。

b) 本従業員は、出願される特許出願のうち自らが発明者であるものについて、インド特許法様式１による宣言の項目に署名し、かつ、それが方法の如何を問わず、雇用主が求める事項において雇用主に協力するものとする。

4. 発明とその帰属

a) 本従業員は、雇用主たる当社が、職務発明の所有権を含むすべての権利を常に有することを了解し、認める。

b) 本従業員は、発明が...の特定の事業分野のみならず、雇用主との雇用期間中に発生するその他の発明も対象とすることを理解する。 これは、インド法に基づく労働契約に従うものであり、それにより雇用主は、本従業員に割り当てられた職責にかかわらず、結果として生じるすべての知的財産を所有することができる。

c) 本従業員は、以下における、現在利用できるか利用できる可能性があるすべての権利、権原及び権益（すべての知的財産権を含むが、これらに限定されない）を、取消不能の形で、永久に雇用主に譲渡する。（a）雇用主のあらゆる知的財産、及び（b）雇用主との提携の一環とし

て、雇用主に対して本従業員が考案、創出、改良、開発、又は提供したあらゆる専有情報。

d)　当社が、本従業員が本契約に基づいて作成又は提供した対象発明又は対象著作物を使用又は利用するにあたり、本従業員が保有する他の財産権に基づく本従業員からのライセンスが必要である場合、本従業員は、本契約により、当該対象発明又は対象著作物の製造、使用、販売、複製、改変、二次的著作物の作成、公開、配布、実行、展示その他の利用するための、支払い済み、ロイヤルティフリーの、非独占的な、永久的な、全世界を対象としたライセンスを、無制限のサブライセンス権とともにここに当社に付与する。当社は、対象発明又は対象著作物に関する全般的な権利を自由に移転又は譲渡することができる。

5. 発明者の義務－発明の開示

a)　発明をなした本従業員は常に、遅滞なく、自身の発明を雇用主に通知しなければならない。発明者の通知義務は、雇用期間中及び雇用終了後２ヵ月間に発生するすべての発明を対象とする。

b)　本従業員は、常に文書又は電子的に雇用主に情報を提出することを了解し、これに同意する。理解してもらえるように、発明の詳細を十分に記載しなければならない。発明の開示にあたっては、以下の短い説明を含める必要がある。

・　既知の技術及びその問題

・　発明及びその利点（上記の問題の解決方法）

・　発明の具体例

・　発明を添付の所定の発明開示様式に記載する

c)　本従業員は、発明の開示にあたり、発明に創造的なインプットを提供したすべての人物を過不足なく特定しなければならないことを了解する。複数の発明者が存在する場合は、発明に対する寄与の程度を記載しなければならない。それぞれの寄与の程度が記載されていない場合は、すべての発明者が発明に対して同等の寄与を行ったものとみなされる。

d)　本従業員は、本従業員が第三者の知的財産権を侵害しておらず、また今後も侵害しないことを表明し、保証するとともに、雇用期間中に第三者の知的財産権を侵害しないことに同意する。

e)　本従業員は、雇用及び当社が本従業員に支払う対価が、本契約の条件によって拘束される、適切で、価値があり、かつ十分な対価であることを認める。

f)　本従業員は、雇用主と協力して、知的財産に関する必要な情報及び登録の完全な手続きを開示することを約束する。これには、その職務終了後に「異議なしの証明書（NOC)」を提出することが含まれる。

6. 秘密保持義務

a)　本従業員は、発明開示が検討中である間、発明者が、雇用主の書面による承諾なしに、発明が公知となる可能性のある情報を開示しないことを約束する。　雇用主はまた、発明開示についても秘密に取り扱う。

b)　本従業員は、発明が、形式を問わず文書で公表され、形式を問わず公に展示され、形式を問わず会議で発表され、形式を問わず公に実施され、形式を問わず公に使用され、口頭又は書面を含めて形式を問わずいずれかの者／第三者に伝達された場合、本発明は、公知であると理解されることを了解する。

7. 発明の管理

本従業員は、雇用主が発明を管理する以下のプロセスを認め、了解する。

a)　発明開示を受領した場合、当該発明について責任を負う知的財産権の管理者／責任者は、発明開示が十分に開示されていることを正式に確認するものとする。

b)　発明開示が不完全であるか又は理解可能なものでない場合は、発明者に返却し、必要な追加を求めるものとする。発明開示は、欠落情報が提出された後にのみ受領されたものとみなされる。

c)　発明者はまた、インド特許法に基づく譲渡又は様式１により、発明を雇用主に譲渡する。

d)　発明に対する権利が雇用主に移転された後、雇用主は、発明の保護及び利用について、自己の最善かつ単独の裁量で決定する。例、雇用主は、特許を出願し、発明を営業秘密として取り扱い、発明を第三者に譲渡し、又は保護を放棄することができる。異なる発明開示を同一の保護の範囲内で組み合わせることも、これが、例えば、より効果的な保護を得ること、又はその他の理由により適切である場合には、可能である。

e)　発明者は、雇用主に対し、その発明に関する必要な文書及び情報を提供し、発明の保護の申請及び維持を支援する義務を負うものとする。請求があり次第、発明者は、すべての譲渡及び譲渡書類（もしあれば）及び出願に関するその他の書類に速やかに署名するものとする。

8. 発明の公知化

本従業員は、すべての職務発明がその事業上の秘密とみなされることをここに認め、了解する。それらを保護するのではなく公表するとの決定は、雇用主が行うものとする。

9. 特許性のないアイデア

a) 本従業員は、当社の事業分野に属するが、特許によって保護することはできないアイデアが、本質的に、追加の措置なしに、…の財産であることを認める。

b) 本従業員は、いかなる状況においても、当該情報を公衆又はいかなる当事者にも開示／共有しないことに同意する。

10. 特許及び著作権の登録

本従業員は、知的財産における雇用主の所有権の担保として必要な著作権及び特許を取得するために、本契約において雇用主にできる限り合理的に全面的に協力することに同意する。この協力は、雇用期間中及び雇用終了後も継続する。

11. 随意雇用 (Employment at Will)

本契約に署名することにより、本従業員は、雇用主との雇用が随意に継続することを了解し、これに同意する。したがって、本従業員の雇用は、正当な理由の有無を問わず、通知の有無を問わず、いつでも、雇用主／本従業員の選択により終了することができ、雇用主は、理由の有無を問わず、通知の有無を問わず、いつでも、すべての場合に本契約のその他の条件に従って、本従業員の雇用のその他のすべての条件を終了又は変更することができる。この随意の関係は、雇用主／…での本従業員の雇用期間中、有効に存続する。本項に定める本従業員の雇用の随意性は、当該性質を明確に変更する旨の、本契約の両当事

者が署名した合意書によってのみ変更することができる。

12. 秘密保持

本従業員は、本契約の過程において、又は本契約に関連して、雇用主から受領したすべての情報を、両当事者が[●]に署名した秘密保持契約に従い秘密として取り扱うことを約束する。なお、当該秘密保持契約の写しは、本契約の付属書[●]として同封される。本契約と秘密保持契約との間に矛盾が生じた場合、秘密保持契約のそれに対応する条項が優先するものとする。

13. 期間

a. 本契約は、締結日から有効になり、拘束力を有するものとし、当社と本従業員の雇用期間の最終日まで有効に存続するものとする。

b. 本契約の終了後、雇用主は、本契約における雇用主のための本従業員の業務に起因又は関連する、雇用終了後の本従業員のすべての知的財産に対する独占的所有権を取得する。

14. 終了

a. 次の場合、雇用主は直ちに本契約を終了することができる。

(i) 本従業員が本契約に基づく重大な義務に違反し、書面による通知があったにもかかわらず、当該通知の日から[・]日以内に当該違反を是正しなかった場合。

(ii) 雇用主の合理的な見解により、従業員の地位、権利又は利益に悪影響を及ぼし、本従業員の解雇を義務付けるような雇用主の支配の変更があった場合。

(iii) 雇用主は、雇用主での本従業員の雇用期間中いつでも、理由を挙げることなく、本従業員に[・]日前の通知を発行することにより、本契約を終了する権利を有するものとする。

b. 本条に基づく終了と同時に、当該終了の時点で本契約に基づき本従業員が履行し、承諾された業務に対して支払うべきすべての支払いは、雇用主が本従業員に対して行うものとする。これは、当該早期終了の場合における雇用主の唯一の救済措置とする。ただし、当該対価は、(i) 本契約に基づいて履行される業務の前払いとして支払われた金額、及び (ii) 本契約の規定によるその他の控除額（もしあれば)、に対する控除／調整の対象となるものとする。

c. 雇用主は、本従業員が本契約に関する秘密情報を雇用主／...の競合他社に開示することが判明した場合、直ちに本従業員の業務を停止する権利を常に有するものとする。雇用主が書面で別段の合意をしない限り、当該停止により、本従業員が追加の対価を受け取る権利を有するわけではない。

15. データ及び文書の返却

本従業員は、本契約の終了後、雇用主の命令に従い、知的財産のすべての有形の具現化物を直ちに返却することに同意する。これには、雇用期間中に開発される、又は開発された図面、文書、データ及びメモが含まれるが、これらに限定されない。本従業員はまた、有形の具現化物のコピーを作成せず、再現を試みず、第三者と共有しないことに同意する。

16. 法と紛争解決

a) 本契約は、インド法に準拠する。

b) 紛争は、以下のとおり解決されるものとする。

i. 本契約に起因又は関連して紛争が生じた場合、当該契約について雇用主の責任ある代表者は、公正な対応と誠意を持って、当該紛争を解決しようと試みるものとし、一方の当事者の要請があれば、雇用主の経営陣の代表が

交渉に参加するものとする。両当事者は、両当事者間に生じたすべての紛争を友好的に解決するよう努める。各当事者は、いつでも相手方当事者に書面で通知することにより、当該交渉を終了する権利を有するものとする。両当事者が、紛争の存在を書面で相互に通知し、かつ、紛争を解決し、会合し当該紛争を解決する提案を送達してから 30 日以内（又は両当事者間で相互に合意するさらに長い期間内）に紛争を解決することができない場合、当該紛争は仲裁に付託されるものとする。

ii. 本契約に起因又は関連する紛争であって、両当事者が第 13 条（b）（i）に基づいて解決することができない紛争（その存在、有効性又は終了に関する疑問を含む）は、当面有効な仲裁及び調停センターの仲裁規則に従い、1996 年仲裁及び調停法により処理される仲裁に付託され、最終的に解決されるものとし、当該規則は、本条において言及することにより組み込まれるものとみなされる。

iii. 仲裁廷は、１名の仲裁人（「仲裁廷」）で構成するものとする。

iv. 仲裁地は、カルナータカ州バンガロールとし、英語で行われるものとする。仲裁廷の決定は、最終的かつ拘束力を有するものとし、裁判所の判決として管轄権を有する裁判所において執行可能であるものとする。それにより、両当事者は、当該執行に対する異議又は免責の申し立てを放棄する。仲裁の費用は、両当事者間で均等に分担するものとする。

v. 仲裁人は、書面及び理由を付した仲裁判断を提供するものとする。

vi. 上記第 13 条（b）（iv）に基づき、司法介入が可能な場合は常に、カルナータカ州バンガロールの裁判所が専属管轄権を有する。

vii. 紛争又は仲裁が係属しているにもかかわらず、雇用主が別段の指示をしない限り、本従業員は、本契約に従って継続して義務を履行するものとし、履行しない場合は、本契約の違反として取り扱われるものとする。

viii. 仲裁により解決された紛争は、秘密扱いとする。秘密保持の対象には、仲裁中に共有されるすべての情報、及び仲裁に関連する和解、決定又は評決が含まれる。本項に基づく秘密情報は、相手方当事者の書面による承諾なしに、いかなる形態においても第三者と共有してはならない。ただし、各当事者は、当該紛争に関連して、相手方当事者に対する適用法に基づく自己の権利を保護するために必要な情報を共有する権利を有する。また、法律、公的機関、証券取引所又は類似の機関に従い、当該情報の開示が義務付けられる場合にも、かかる情報を共有する権利を有する。

c) バンガロールの管轄裁判所は、本契約に起因又は関連するすべての紛争について専属管轄権を有するものとする。

17. 譲渡

i. 両当事者は、本契約における責任を第三者に譲渡しないことに合意する

ii. 本従業員は、雇用期間中に創出され、及び／又は発見されたすべての知的財産に対する現在及び将来のすべての権利及び権原ならびに権益を雇用主に譲渡することに同意する。

18. 可分性

本契約のいずれかの条項が、管轄権を有する裁判所により無効、有効性なし及び執行不能と判示された場合であっても、残りの条項は影響を受けない。両当事者は、無効又は執行不能な条項を、両当事者の意図を最大限可能な方法で満たす有効かつ執行可能な条項に置き換えることをここに約束する。本契約の抜け穴についても同様のことが適用され、両当事者の意図に従って実施されるものとする。

19. 完全合意

本契約は、本契約の主題に関する本契約の両当事者間の完全な合意及び了解事項を含み、明示・黙示を問わず、本契約の主題に関するあらゆる性質のすべての従前の合意、了解事項、誘因及び条件に取って代わる。本契約の明示的な条件は、本契約の条件のいずれかに合致しない履行の過程及び／又は商慣習に優先する。

20. 承継人及び譲受人

両当事者は、雇用主ならびに雇用主の相続人、承継人及び譲受人の利益のために、本契約が本従業員の相続人、承継人及び譲受人を拘束することに合意する。

21. 修正

両当事者は、本契約に対する修正が、両当事者が本契約に署名しなければならない場合、書面によらなければならず、両当事者が行った当該修正のみが本契約に適用されることに合意する。

22. 署名及び日付

両当事者は、ここに、本契約に定める条件に合意し、当該条件は、下記の署名により実証される。

以上の証として、本契約の両当事者は、上記の日付で本契約を締結した。

従業員	雇用主
氏名：_____	氏名：_____
署名：_____	署名：_____
日付：_____	日付：_____

（3） 販売契約書

本契約（「本契約」）は、_____［日付の挿入］に以下の者の間で締結される。

契約当事者

一方当事者として、_____［ベンダー／サプライヤー／製造業者の名称及び住所を挿入］（以下「**売主**」といいい、この表現は、文脈又はその意味と矛盾する場合を除き、その承継人、譲受人、パートナー、法定相続人、代表者を意味し、これらを含むとみなされるものとする）。

及び

他方当事者として、_____ に登録事務所を有する_____［会社名の挿入］（以下「**買主**」といい、この表現は、文脈又はその意味と矛盾しない限り、その承継人、譲受人、パートナー、法定相続人、代表者を意味し、これらを含むとみなされるものとする）。

両当事者は、個別には「当事者」といい、総称して「両当事者」という。

売主は、_____（ベンダー／サプライヤー／製造業者の詳細）の委託製造業者である。

買主は、製薬会社／_____であり、本契約に記載される買主の仕様に従い、商品（以下「**商品**」）の製造を売主に打診した。

以上より、本契約に定める約束及び約定を約因として、ならびにその他の有効かつ有価の約因により、両当事者はここに、以下を遵守することに合意する。

本契約の両当事者は、以下を遵守することに合意する。

売主の義務

1. 売主は、売主の業界において実践され、受入れられている最良の技術ノウハウ、注意、及び技能を使用し、また、有効なすべての適用法令を遵守して、指定された商品を製造することに同意し、これを約束する。
2. 売主は、買主が注文する指定の商品を製造するための適切な製造施設を有しており、買主が提示する仕様に合致する当該商品を、買主が提示する期間内に製造することができることを確認する。
3. 売主は、商品の生産のために、良質な材料を購入することに同意する。
4. 売主は、買主が注文商品のすべての所有権を維持することに同意する。売主は、買主の明示的な許可なく第三者に商品を販売することは許可されない。
5. 売主は、直接もしくは間接的に、又は第三者を通じて、製造された商品を消費者に販売しないことに同意する。
6. 売主は、自己の事業に適用されるすべての現地及び外国の法令を遵守することに同意する。

知的財産権

1. 売主は、ブランド、ロゴ、タグライン、商標、特許、サービスマーク、営業秘密、著作権及び意匠、又は本契約に明示的に記載されていないその他の知的財産を含む、買主の知的財産権の唯一の保有者であることを確認し、これに同意する。買主は、買主の知的財産が第三者の知的財産を侵害しておらず、又は、それらに違反していないことを、表明し、保証する。
2. 本契約の条件に基づき、買主は、本契約が有効である間、商品を製造するために買主の知的財産を使用するための、限定的な、譲渡不能の、非独占的ライセンスを売主に付与する。

3. 売主は、一見類似する、又は混同を惹起する可能性のある、買主の知的財産によく似た商標、サービスマーク又はトレード・ドレスを登録しないものとする。
4. 買主が付与した限定的ライセンスは（もしあれば）、本契約の終了時に満了する。
5. 製品を製造するための再委託／サブライセンスは、買主の書面による正当な許可を得なければならず、当該再委託は、買主のための知的財産権の独占的所有を維持できるように、本契約に定めるのと同じ条件及び条項に従うものとする。

価格及び支払い

1. 商品の購入単価（「購入価格」）は、下記のとおりとする。
    a. ____INR（インドルピー）
2. 発注する商品の数量は、下記のとおりとする。
    a. ____
3. 売主は、買主に請求書を提供するものとし、買主は、請求書の日付から____日以内に、その一部（支払総額の 50%）を支払うものとする。
4. 購入価格は、インドルピー（INR）で支払うものとする。
5. 購入価格には、買主が支払うことに同意する、送料、製品保険又はその他取扱手数料が含まれるものとする。
6. 買主は、____あたり_____インドルピーの価格で、かつ買主の提示した技術仕様に基づく_____の商品（以下、「当該商品」）を売主から購入することを約束する。

商品の引渡し

1. 両当事者は、本契約に基づく売主の履行において、期限厳守であることに合意する。商品の全部は、2021 年_____までに引き渡されるものとする。指

定引渡日までに商品の引渡しが行われない場合、又は買主が提示する仕様に従った引渡しが行われない場合、買主は、本契約を重大な違反として取り扱い本契約を解除するか、又は適切とみなす他の法的手段を求めるために法的救済を求める権利を有するものとする。

2. 本契約の結果として買主が行った支払いは、売主に送金されるものとし、その後一切支払いは行われないものとする。買主は、本契約を重大な違反として取り扱い、本契約を解除するか、又は自己の裁量により法的救済を求める権利を有するものとする。売主が事前に指定された日程で製造した商品を引き渡さない場合、売主は、商品の引渡し遅延の日数が_____日につき_____%の利息を買主に支払う責任を負う。

商品の検査

1. 商品の引渡し後、買主は、商品の検査のために_____日間を有する（「検査期間」）。検査期間内に商品が仕様に適合しないと買主が判断した場合、買主は、当該検査の日から____日以内に書面で売主に通知するものとする。
2. 売主は、欠陥を是正するために、商品の不適合を売主に通知した日から_____日を有するものとする。
3. 製品の品質保持期限切れを除き、目視検査後に発見された、隠れたる製造上の欠陥（規制当局への申請及び分析証明書の不遵守）であって、それにより契約地域で本製品を販売することが許可されないものは、製品の品質保持期限までの全期間中、買主から売主に通知される。この場合、買主は、売主に通知するとともに、必要に応じて、独立当事者による検査のために買主にサンプルを送付する。

4. 製品の製造上の欠陥又は隠れたる欠陥があり商品が返品される場合であって、法定要件を遵守しないとき、本商品は売主の費用負担で売主に返品されるものとする。

秘密保持

1. 売主は、商品の技術仕様を含め、一定の非公開秘密情報、営業秘密情報（総称して「**専有情報**」）を買主から受領する場合があることを認め、これに同意する。
2. 売主は、専有情報が買主にとって価値があり、すべてのメモ、仕様書、製法、技術仕様書、アルゴリズム、図面又はその他の関連情報を秘密に保持しなければならないことに同意する。
3. さらに売主は、本情報を使用しないこと、及びいかなる第三者にも開示しないことに同意する。売主は、買主が共有するすべての専有情報を買主に返却することとし、売主は、買主の専有情報のコピーを作成しないものとする。

終了

1. 本契約は締結日に開始し、次の日付_____まで存続するものとする。その後、当事者の関係は自動的に終了する。いずれの当事者も、以下に定義される重大な違反を理由に、本契約を終了することができる:
    a. 売主が、指定したとおり引渡しを行わなかったこと
    b. 買主が、支払いを行わなかったこと
    c. 売主が、商品の欠陥を是正しなかったこと
    d. いずれかの当事者の破産

2. いずれかの当事者が本契約に違反した場合、相手方当事者は、10 日前までの書面による通知により終了することができる。当該通知には、違反に関するすべての情報を記載し、違反当事者に対し、その後_____日以内に違反を是正する機会を提供するものとする。当該期間内に違反が是正されなかった場合、本契約は終了する。違反が是正された場合、本契約は引き続き完全に有効に存続する。

法律上の救済

一方の当事者による重大な違反により本契約が解除された場合、非違反当事者は、コモン・ロー及び衡平法上の利用可能な救済を求めることもできる。

紛争解決

性質の如何にかかわらず本証書に起因又は関連して、本契約の両当事者間に紛争又は意見の相違が生じた場合、当該紛争又は意見の相違を、合意のある場合に共通の仲裁人による仲裁に付託するものとし、合意のない場合、２名の仲裁人による仲裁に付託するものとし、各当事者が１名ずつ指名する。当該仲裁人は、主宰仲裁人を指名するものとし、当該仲裁は、1996 年仲裁法及び調停法、又はその修正法に準拠するものとする。仲裁地は、ニューデリーとする。

不可抗力

1. いずれかの当事者が不可抗力（戦争、自然災害、人為的又は自然発生のパンデミック、天災、政治不安などを含むが、これらに限定されない）の影響を受けた場合、当該当事者は、当該不可抗力の性質及び範囲を速やかに相手方当事者に通知するものとする。

2. 本契約に基づく自己の義務の履行遅滞又は不履行が相手方当事者に通知された不可抗力に起因する場合、いずれの当事者も、当該履行遅滞又は不履行を理由として本契約に違反しているとはみなされず、当該義務の履行時期は、それに応じて延長されるものとする。不可抗力が発生したことを相手方当事者に通知せず、又は、相手方当事者への通知が時機を失していた当事者は、当該不可抗力に言及することはできない。
3. 当該不可抗力が継続して３ヵ月を超えて継続する場合、両当事者は、その影響を軽減するため、又は公正かつ合理的な代替的取決めに合意するために、誠意を持って協議を開始するものとする。 両当事者間で合意に達することができず、かつ不可抗力により影響を受けた当事者が当該不可抗力の影響を軽減するためのあらゆる合理的な努力を払わない場合、他の違反に関するいずれかの当事者の他の救済を求める権利を損なうことなく、30 日前の通知をもって、本契約を終了することができる。

総則

1. 本契約のすべての付属書は、本契約の不可分の一部を構成するものとする。
2. 本契約は、インド共和国法に準拠するものとする。両当事者は、法の選択、管轄権、裁判地は任意規定ではなく、本質的に強行規定であることに合意する。
3. 本契約に基づいて行われるすべての通信又は通知は、英語で行うものとする。
4. いずれの当事者も、本契約又は本契約において付与される権利について、その全部又は一部を譲渡、売却、賃貸又はその他移転してはならない。
5. 本契約は、両当事者が署名した書面によってのみ修正されるものとする。
6. 本契約のいずれの条項も、いずれかの当事者の行為又は黙認により放棄されたとはみなされないものとする。 追加の書面による合意のみが、本契約のいずれ

かの条項又は規定の権利放棄を構成し得る。いずれかの当事者が本契約のいずれかの条項を執行しない場合であっても、それが当該条項又はその他の条項について権利放棄をしたことにはならないものとする。

7. 本契約のいずれかの規定又は条項が執行不能と判定された場合、本契約は、その他の点で執行不能な規定及び本契約の残りの部分を有効かつ執行可能にするために必要な範囲で修正されたとみなされるものとする。
8. 本契約は、両当事者間の完全合意を構成し、書面又は口頭を問わず、従前の了解事項に取って代わる。
9. 本契約に基づいて付与される通知は、書面によるものとし、本契約の冒頭に記載される関係当事者の住所宛に書留宅配便又は電子メールで送付されるものとする。

締結

売主		**買主**	
氏名		**氏名**	
役職		**役職**	
日付		**日付**	

［経済産業省委託事業］
インドにおける営業秘密管理マニュアル

2023 年 3 月発行
禁無断転載

［調査受託］
RNA （法律事務所）

日本貿易振興機構 ニューデリー事務所
（知的財産権部）

本冊子は、作成時点に入手した情報に基づくものであり、その後の状況によって変わる場合があります。また、掲載した情報・コメントは著者及び当機構の判断によるものですが、一般的な情報・解釈がこのとおりであることを保証するものでないことを予めお断りします。