

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

はじめに一増補・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、事前の予防治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	6
第1章（基礎知識編）	9
本章のポイント	9
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	9
(1) ショート動画 SNS を通じた営業秘密漏えい	9
(2) 国家機関も警鐘を鳴らす“微信”（We Chat）	10
2. なぜ、営業秘密を保護する必要があるのか	11
3. 中国における営業秘密侵害の典型パターン	13
第2章 法制度編	20
本章のポイント	20
1. 中国における営業秘密の定義	20
2. 法律上の3要件—非公知性・価値性・管理性について	22
3. 中国における営業秘密侵害行為の定義	24
Step Up! リバースエンジニアリング	28
4. 侵害行為に対する救済	29
(1) 民事的救済	31
(2) 行政処分	32
(3) 刑事制裁	32
5. 民事手続きにおける諸制度	34
(1) 立証責任の負担軽減に関する法規定	35
(2) 証拠収集の負担軽減に関する制度—証拠保全	39
(3) 裁判における秘密保護に関する制度	40
6. 営業秘密に関する紛争・事件—参考裁判例	41
第3章 漏えい対策実践編	51
本章のポイント	51
1. 総論	51
(1) 管理体制の構築を考える上での2つの視点	51
(2) 秘密管理性要件充足性の観点からの管理体制の構築	52
(3) 漏えい対策実効性の観点からの管理体制の構築	53
2. 管理体制整備のステップ1—管理体制の現状の確認	55
(1) 現状把握の必要性	55
(2) セルフチェックシート	56

Step Up! 「5つの対策の目的」との関係.....	59
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	60
(1) 営業秘密情報の洗い出し	60
Step Up! 顧客リストの営業秘密該当性	61
(2) 重要度の区分	63
4. 管理体制整備のステップ3－管理体制の整備	63
(1) 担当部門／担当者の設置	63
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...	65
(2) 従業員の管理	66
Tips! 日系企業の管理の実例－営業秘密の分類と取扱いの揭示	67
Step Up! 個人情報保護法との関係	70
Tips! 日系企業の管理の実例－携帯電話と SNS 管理	72
Step Up! 企業版 WeChat	74
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	76
Tips! 日系企業の管理の実例－良好な職場環境の整備	79
(3) 執務室の管理	79
(4) 生産現場の管理	81
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	82
Tips! 日系企業の管理の実例－工場内の掲示物の見直し	83
(5) 取引先の管理（☞ハンドブック P.81～91）	84
5. 漏えい時の対応	87
(1) 漏えいの兆候（☞ハンドブック P.145～147）	87
(2) 初動対応（☞ハンドブック P.148～154）	89
(3) 民事訴訟	90
(4) 行政摘発	91
(5) 刑事摘発	92
(6) 冒認出願の確認	92
(7) 対応フロー	93
参考書式	94
1. 就業規則における秘密保護関連規定の例	94
2. 従業員との秘密保持契約書の例	100
3. 退職後の競業避止契約書の例	104
4. 取引先との秘密保持契約書の例	110
5. 来訪者受付表（中国語版）	117



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ください。

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

い一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 SNS¹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、登録ユーザー数が 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」と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.gbjm.gov.cn/n1/2018/0605/c409095-30037166.html>

³ <http://www.gbjm.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「**朋友圈（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）化学系メーカーの事例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）電機メーカーの事例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。

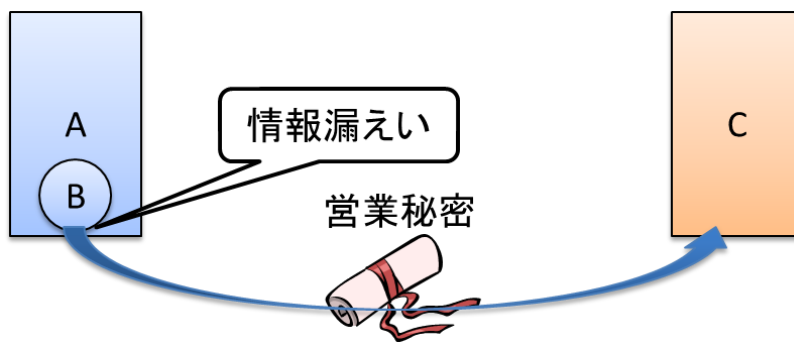
従業員漏えい型は、さらに、次の4つのパターンに分類することができます。

- 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、大手化学メーカー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。）⁶P.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

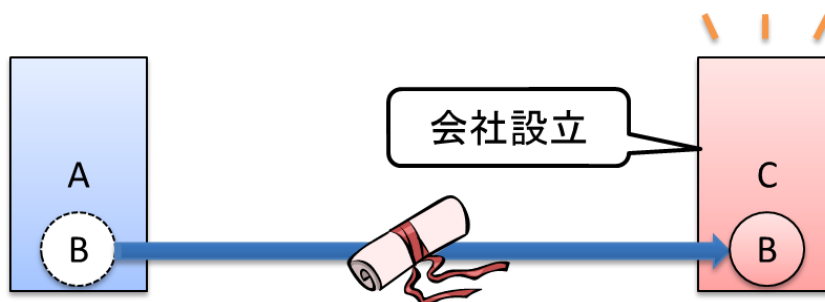
これは、自社（A社）の従業員Bが、A社を退職して競合企業C社に転職し、C社にて前勤務先のA社の営業秘密を利用したり、開示したりするパターンです。



例えば、中国の大手食品メーカー（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ー（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、当該食品メーカーには、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

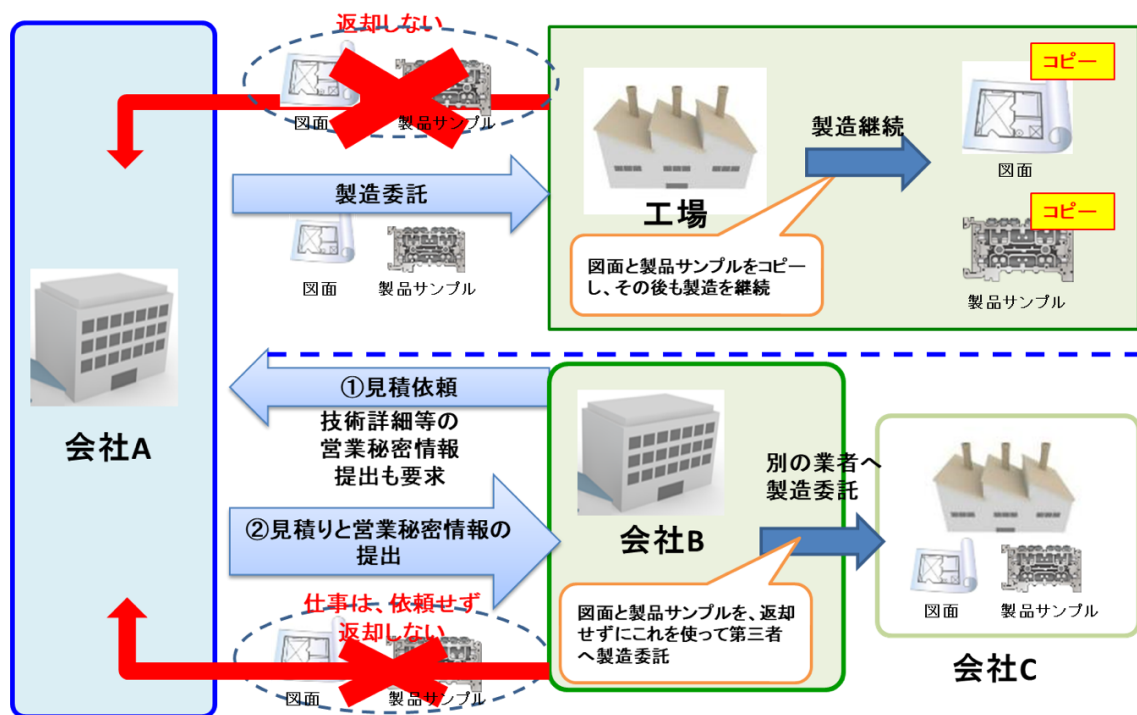
- 従業員が、何が営業秘密に該当するか分かっていない、又は、営業秘密の保護として自分たちが何をやれば良いのか、逆に、何をしてはいけないのかを理解できておらず、ショート動画アプリ等で営業秘密を含むような動画を投稿してしまうパターン
- 従業員が、業務の過程で、WeChat での誤送信等により、誤って営業秘密を漏えいするパターン

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、ライセンサーといった、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、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ー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	反不正当竞争法	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す、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竞争法上の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年の反不正当竞争法の改正により、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出来ます。

(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年の反不正当竞争法の改正により、「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れ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、幫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。

	中 国	日 本
根拠法	反不正競争法（第9条）	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）
不正手段による取得／開示	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 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	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。）
不正開示	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	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

	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・幫助	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、幫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（反不正当竞争法第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 年の反不正当竞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（北京市高级人民法院 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 ・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（市場监督管理局）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。	
--	-------------------------------------	--

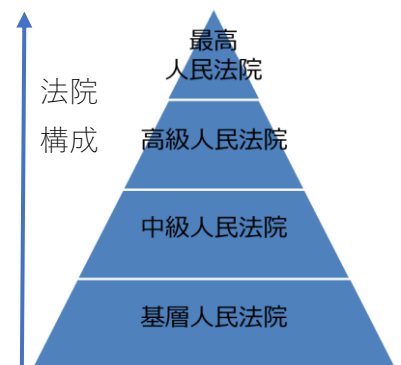
以下、それぞれについて概説します。

(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（反不正当竞争法第 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（反不正当竞争法第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年以下の有期徒刑に処し、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年以下の有期徒刑に処し、かつ罰金を併科する。

※なお、前記各号の行為を知らず、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年以下の有期徒刑及び／または罰金です。情状が特に重大な場合には、3年以上10年以下の有期徒刑に処され、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年以上の有期徒刑を科す場合には、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、最高人民检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、最高人民检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 年の改正反不正当竞争法では、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、効果等を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る、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 1 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、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る、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（反不正当竞争法第 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

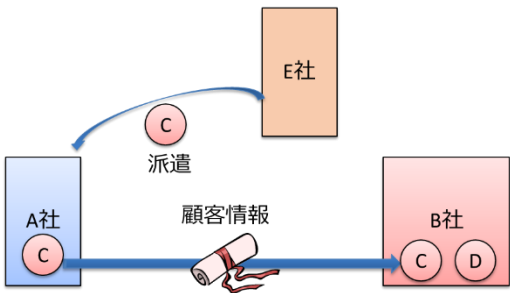
¹³ 2021 年改正前の民事訴訟法 111 条の規定であり、執筆時点で有効な民事訴訟法における対応規定 114 条には、例えば、暴力等の手段により司法職員の業務執行を妨害した場合等において、人民法院は罰金等を科すことができる旨、規定されています。

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

	一審被告	C 社、D 社、E 社
		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ーであり、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。
--	---

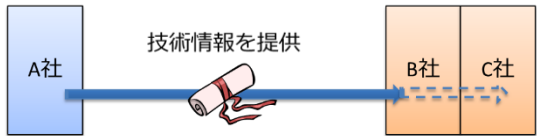
✎ポイント

- 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

基本情報	裁判所／ 審級	最高人民法院／第二審	
	事件番号	(2020) 最高法知民終 621 号	
	判決年月 日	2021 年 12 月 18 日	
	一審 原告	A 社	
	一審 被告	B 社	C 社
経緯	 ・ 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。		

	・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 社の違法行為を知らながら 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、現行の反不正当竞争法の第 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い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。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區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、地域的な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。



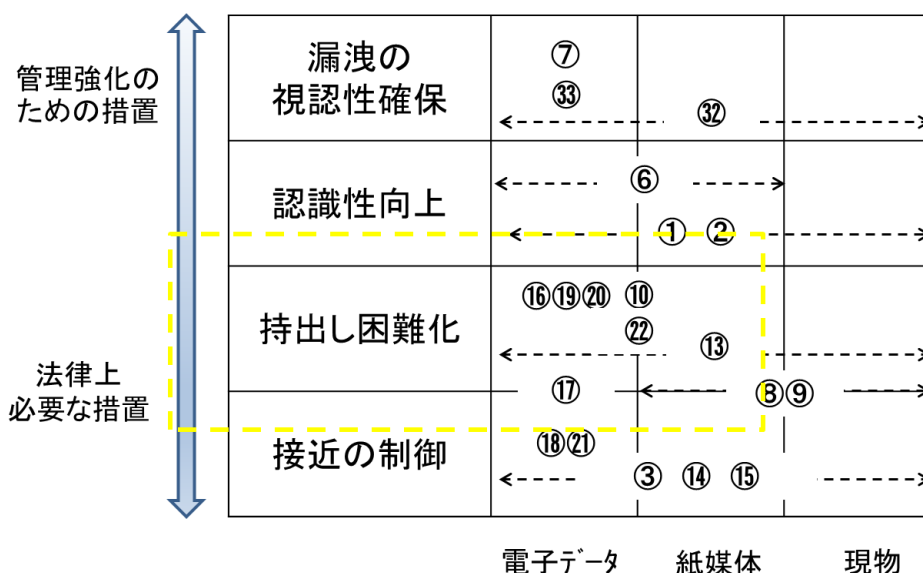
Step Up!

「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」(P5)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 P10～27)

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いいでしょう。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。

技術情報

- 技術に関する構造、原料、成分、レシピ、材料、サンプル、型式、植物新品種繁殖材料、工法、方法またはその手順、アルゴリズム、データ、コンピュータプログラム等

経営情報

- 経営活動に関するアイデア、管理、販売、経理、計画、見本、入札資料、顧客情報、データ等



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、「一般的なりストであり、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。粒度が大きすぎると（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ります。

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のでしょうか。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い良いでしょう。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い良いでしょう）
- 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揭示

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元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○、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。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い良いでしょう。

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い良いでしょう。

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）。



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1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。

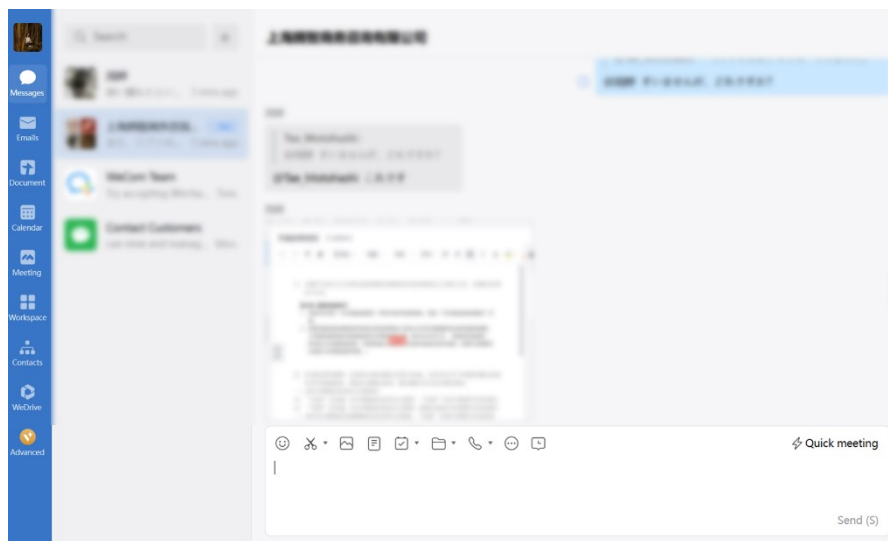
- ・ WeChat で送受信できる情報は、営業秘密にかかわらない情報に限定し、営業秘密情報は、上長の事前の許可がない限り、メールでパスワードをかけて送受信すること
- ・ 工場内でも、WeChat による営業秘密にかかわる情報の送受信は、原則として禁止する。緊急時には、必要かつ最小限の範囲で、営業秘密にかかわる情報を上長に対して送受信することができるものとするが、その情報が必要なくなった時点で、または、上長の指示に従い、全ての送受信者が当該情報を速やかに削除すること



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 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1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、E S²¹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、社員とその家族と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、E S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E S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（持ち出し／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。

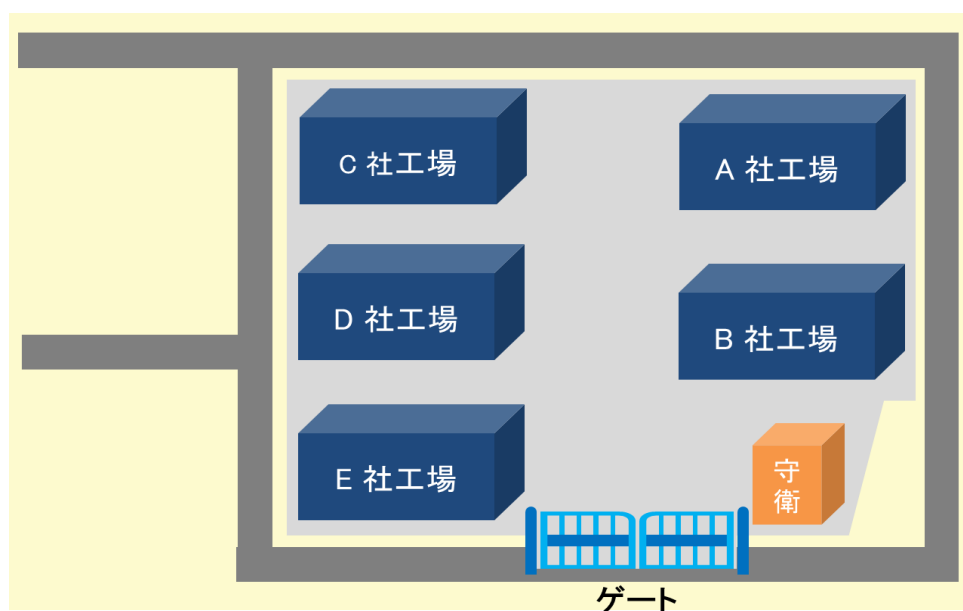
また、裏紙を利用している企業も多いと思われますが、営業秘密保護の観点からは、できれば裏紙利用を禁止したいところです。裏紙利用を認める場合には、上述した「日系企業の管理の実例－営業秘密の分類と取り扱いの揭示」のように、部署単位で具体的に何が営業秘密に該当するか、確実に理解を共有し、営業秘密が裏紙として安易に再利用、廃棄されることを防止する必要があるでしょう。

（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、「工業園區」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。工業園區によっては、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區の場合、下図のように、敷地内に複数の会社の工場が、仕切塀などが無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。



工業園區の例

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を行われておらず、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いますが、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せんが、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、ライセンサ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。下請けやライセンサーについては、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、下請けやライセンサーに対しては、必要に応じて、情報管理についての監査・指導を受け入れること（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、「たとい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りますが、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 P148～150）

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員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 P C 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かかわらず急激な浪費をし始めた
 - ex) 頻繁に特定の競合他社と接触している

※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ち切り
ex) 自社しか製造できないはずの特別な部品について、発注元からの部品発注が途絶えた
- ・ インターネット上での取引先に関する噂
ex) インターネット掲示板、SNS、HP 等において、自社の非公開情報や自社製品との類似品が取り沙汰されている
- ・ 取引先からの、取引内容との関係では必ずしも必要でないはずの業務資料のリクエストや通常の取引に比べて異様に詳細な情報照会
- ・ 自社の秘密情報と関連する取引先企業の商品の品質の急激な向上
- ・ 自社の秘密情報と関連する分野での取引先の顧客・シェアの急拡大

※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 年の改正反不正当竞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 P C や U S B 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が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。

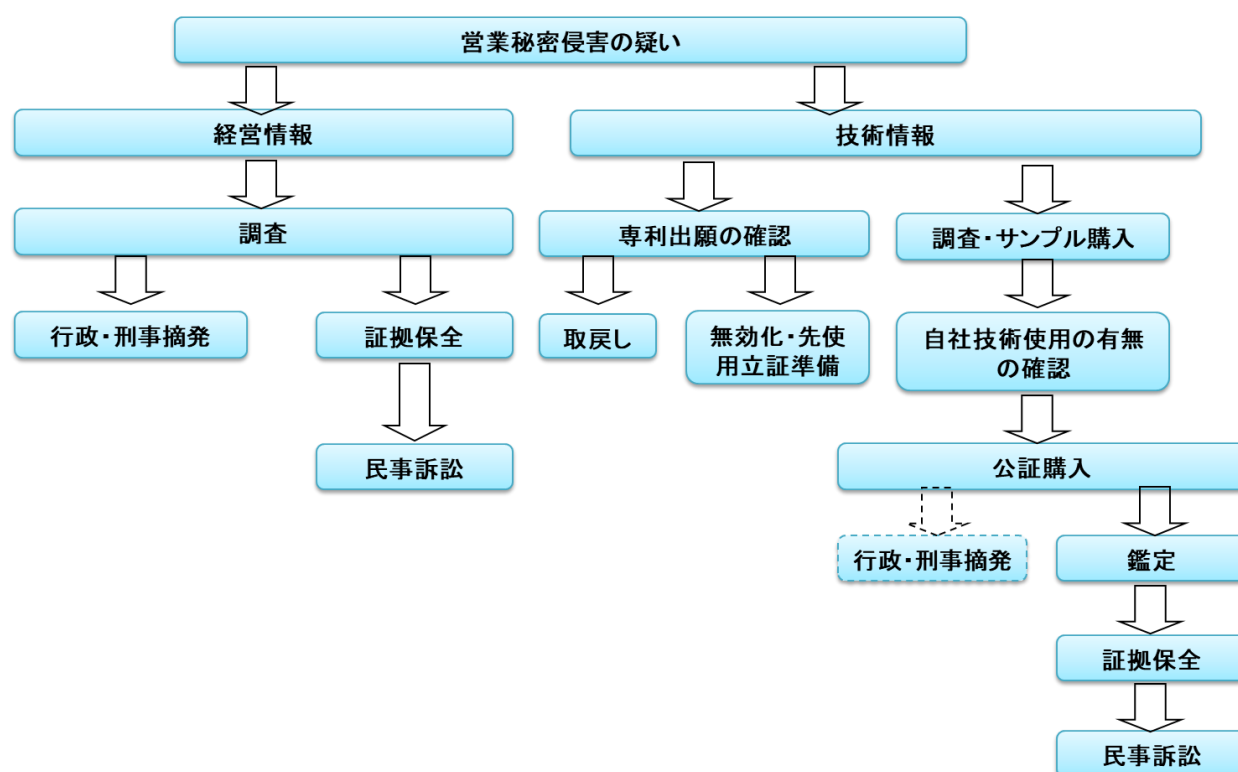
（6）冒認出願の確認

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わってきます。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密义务。
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ない。会社は、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ない。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. 退職後の競業禁止契約書の例

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、联系方式、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こと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
--	--

N O	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	

××有限公司 出入記録

				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。 * 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					
				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。					
N O	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、本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