

2021年11月2日

企業の中国におけるビジネス秘密保護

顧問・中国特許弁理士
鐘 晶 (Zhong Jin)



ビジネス秘密(Business Secret)は企業の核心情報である。経済社会の発展と市場競争が激しくなると伴い、企業のビジネス秘密、特にその中の技術秘密の重要性がますます顕著になる。ビジネス秘密保護は、直接企業自身の経済利益と発展利益に関係しており、企業の競争優位性の維持と強化にも関係しており、真剣に管理し、重点的に保護しなければならない企業の知的財産権である。

近年、中国はビジネス秘密保護に関する法律法規を絶えず完備し、保護力も強化していき、民法保護、行政法保護、刑事保護を含むビジネス秘密法律保護体系を構築した。今年2月、最高人民法院は、嘉興市中華化工有限責任公司などと王龍集团有限公司などの「バニリン」技術秘密侵害紛争上訴案件に対して判決を下し、被疑侵害者の王龍集团公司などが技術秘密権利者に1.59億元を賠償すると判決した((2020)最高法知民終1667号)。情報によると、この事件は、これまで中国の裁判所が下した発効の判決のうちに、賠償額が最も高いビジネス秘密侵害事件である。最高人民法院所知的財産権法廷の2020年度10件技術系知的財産権の典型案例の一つとして、裁判所は、当該事件の判決を通じて、法によって重要産業の核心技術を保護し、悪意のある権利侵害に対する打撃力を確実に強化し、人民裁判所が厳格に法によって知的財産権を保護し、悪意のある権利侵害行為を厳しく打撃するという鮮明な司法態勢を示した。

司法レベルで保護と処罰を強化し、ビジネス秘密が侵害された場合、企業はいくつかの司法救済ルートを通じて権利を保護することができるが、ビジネス秘密が一旦漏れてしまったら、企業のビジネス秘密の権利と価値が失われてしまい、企業に取り返しのつかない損害を与え、企業の生存と発展にも影響を与

える。このため、企業は予防策を講じて、ビジネス秘密保護を確実に行うべきである。ビジネス秘密保護について、企業は、2つの方面の措置を重視するべきである。1、企業内部のビジネス秘密管理と保護を確実にすること； 2、権利侵害発生可能なことへの早期警報と対応を確実に行うこと。

一、企業内部のビジネス秘密管理と保護について

企業内部のビジネス秘密管理と保護を確実にしようとする場合、まず、ビジネス秘密の意味のある特徴を理解するべきである。『中華人民共和国反不正競争法』（以下は『反不正競争法』と略称）第九条の規定により、ビジネス秘密とは公衆に知られておらず、商業的価値を有しかつ権利者が関連の秘密保持措置を取った技術情報、経営情報等の商業情報をいう。法律の規定から見ると、ビジネス秘密は企業に現実的または潜在的な経済的利益と競争優位をもたらすことができる技術情報と経営情報を含み、秘密性、価値性、秘密保持性という3方面の特徴を持っており、これはビジネス秘密の構成要件に対する法律の規定である。

ビジネス秘密の特徴の中の秘密性、価値性のいずれも情報自体が持つ特性であるが、秘密保持性は権利者が別途に秘密保持措置を取って情報に付加した特性である。合理的で効果的な保護措置がとられていない場合、その情報は秘密保持性を有さず、その情報は法的に認められたビジネス秘密とは考えられない。これからわかるように、企業が自分のビジネス秘密に対して秘密保持措置をとっているかどうかは非常に重要である。厳格な秘密保持措置は、事件発生の前にビジネス秘密が侵害を受けることを有効に予防するだけでなく、事件発生後の紛争において、通常、裁判所は、当該情報がビジネス秘密の構成要件を満たしているかどうかを判定し、ビジネス秘密の認定は、裁判所がビジネス秘密事件を審理する際の必須手続きで、構成要件の判定において、秘密保持性がよく争議の焦点となる。企業が主張するビジネス情報のいずれも裁判所にビジネス秘密として認定されていなければ、当該ビジネスへの保護を主張することができない。また、秘密保持措置を取っても、企業が十分に証明できない場合は、立証不能ということの不利な結果を負担し、敗訴になる。このため、企業内部のビジネス秘密管理と保護には、関連ビジネス情報に対する合理的かつ効果的

な秘密保持措置を取ることがポイントである。

『最高人民法院による不正競争民事案件の審理における法律応用の若干問題に関する解釈』（以下は『解釈』と略称）第十一条において、「人民裁判所は、情報の媒体の特徴、権利者の機密保持の要望、機密保持措置の識別の程度、他人が正当な方法を通じて得る難易度等の要素に基づき、権利者が機密保持措置を講じているか否かを認定しなければならない。

次の各号のいずれかに該当し、正常な状況下で機密に関わる情報の漏えいを防止するに足りる場合は、権利者が機密保持措置を講じていると認定しなければならない。

（一）機密に関わる情報を知る範囲を限定し、知る必要のある関係者についてのみ、その内容を告知する。

（二）機密情報に関わる媒体に鍵を掛ける等の防犯措置を採る。

（三）機密情報に関わる媒体に機密保持の表示を付す。

（四）機密に関わる情報にパスワードやコードを使用する。

（五）秘密保持契約を締結する。

（六）機密に関わる機械、工業、生産現場等の場所への来訪者を制限し、又は秘密保持を要求する。

（七）情報の秘密を確保するその他の合理的な措置。」と規定されている。

具体的には、企業は少なくとも以下の機密保護措置を取るべきである。

1. 企業のビジネス秘密の範囲を明確にし、定密と識別を行う。

定密とは、ビジネス秘密のレベルを分けることを指す。機密情報に対して、科学的に分級分類を行い、レベル別の管理措置を施す。核心ビジネス秘密については、永久または期間限定無しの保護レベルを採用し、接触者をリーダーレベルと核心技術者レベルに制限しなければならない。一般的なビジネス秘密については、長期的な保護レベルを取ることができ、接触者を技術部門と関連スタッフに緩和することができる。低レベル、臨時的なビジネス秘密については、必要な秘密保持期間に応じて、短期または定期的な保護レベルを採用し、接触者も必要な業務人員までに緩和することができる。

識別とは、ビジネス秘密を明らかに識別しやすい方法で義務者に周知させることである。最もよく使われている方法は、関連秘密情報に対して、秘密を表示することであり、すなわち、開示、周知しやすい方法で、当該情報がビジネス秘密であることを表明する。主な対策としては、紙の機密文書に対して表紙には「密」を表記する方式、電子版の機密文書に対して透かしの方式で、ビジネス秘密情報であることを表明する；機密に関与する場所において、表示板で「機密場所、従業員以外は立ち入り禁止」と表示する等；会社規定、公告通知などの開示文書にビジネス秘密の範囲を具体的に明記する；新たに形成され、明確にされていないビジネス秘密については、決議、公告などの方式で適時に義務者に周知させる。

2. 企業秘密保持制度を確立し、秘密保持措置をとる。

秘密保持制度には、社内の従業員に対する規定を制定するだけでなく、社外への秘密保持要求も考慮しなければならない。

社内への制度は主に(1)従業員に秘密保持教育を実施し、全従業員に秘密保持措置を守るように教育すること；(2)秘密関与の従業員と、秘密保持契約と競争制限契約とを締結し、契約の条項には従業員の秘密保持義務と秘密保持の範囲とを具体的に明確にすること；(3)社員の入社・離職の背景を追跡して確認することを含む。

社外への秘密保持要求は主に(1)訪問者登録制度の実施と秘密保持要求の提出、(2)対外商業交渉と契約締結時の秘密保持要求を規定し、秘密保持の最低ラインを規定することを含む。

常用の物理的な措置は以下のとおりである。(1)オフィスに秘密保持エリアを設ける。秘密保持エリアを区分すること、身分識別システム、シームレス監視システムなどを利用することにより、ビジネス秘密保管場所の物理的安全を保證する。(2)秘密情報に対して、暗号やコードを用いる。(3)秘密情報の媒体に対してロックをかけるなどの防犯措置をとる。異なる媒体のタイプと秘密保持のニーズに応じて、サーバー格納、独立保存、非電子化保存などの方式をそれぞれに選択して保管して、格納情報が永遠に安全に保存されており、バックアップ情報が有効に更新され、一時的な格納情報が適時に削除されて廃棄され

ることを保証する。同時に、秘密保持の格納範囲から撤退する秘密関与記憶装置、リムーバブルストレージ媒体に対して秘密解除を行い、もう使用しない秘密関与の非電子化の保存文書、書き込みディスクなどを廃棄するように注意する。

3. 企業のソフト、ハードウェア管理を完備し、保管と痕跡の残しをしっかりと行う。

法律の規定によると、ビジネス秘密を主張する原告は、機密保持措置を行ったことを証明する責任を負い、機密保持措置を行っただけで証明できなかった場合には、事後に機密保持措置をしていなかったと依然として認定される。保管と痕跡を残すとは、企業がすでにとった機密保持措置に対して証拠を保留することで、事後の立証を容易にする。具体的な方法は主に以下のことを含む。(1) ファイル制度を整備し、会社が制定した秘密保持規定及び従業員と締結した秘密保持契約書と労働契約書の原本を適切に保管すること。(2) 秘密保持教育活動を記録又は録音録画すること。(3) コードや暗号を用いた秘密情報について、コードを使用する目的がビジネス秘密保護で、日常業務上の便宜のためではないことを明確に説明すること。(4) 執行した機密保持措置は記録と秘密保持マークを保留すること。

もちろん、上記の方法と措置は企業のビジネス機密保持措置の常用手段だけであり、企業内部のビジネス秘密管理と保護はシステムプロジェクトであり、企業全体の知的財産権保護方針に基づいて、細かい管理制度、科学的な社員管理、厳密な情報管理及び明確な職責分業などの面から構築しなければならない。

二、権利侵害発生可能なことに対する企業の早期警報と対応について

権利侵害発生可能な際の企業の早期警報と対応は、内部での健全な保護管理体制の基礎、発生可能な侵害行為を対応するために構築されたものである。その役割は、侵害の兆候を早期に発見し、救済案を制定し、権利行使措置を実施し、侵害行為の継続的な発生を停止し、企業の損失を最小限に抑えることである。『反不正競争法』第9条の規定により、事業者は、次の各号に掲げるビジネス秘密に係る侵害行為を実施してはならない。

(1) 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ビジネス秘密を獲得すること。

(2) 前号に定める手段を用いて獲得した権利者のビジネス秘密を開示、使用し又は他人に使用を許諾すること。

(3) 秘密保持義務又は権利者のビジネス秘密保持に関する要求事項に違反して保有しているビジネス秘密を開示、使用し、或いは他人に使用を許諾すること。

(4) 秘密保持義務又は権利者のビジネス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、幫助して権利者のビジネス秘密を獲得、開示、使用し又は他人に使用を許諾すること。事業者以外のその他の自然人、法人又は非法人組織が前項に掲げた違法行為を実施する場合は、営業秘密を侵害する行為とみなされる。

『解釈』第十四条の規定により、企業のビジネス秘密が侵害されていることが判明した場合、当事者が、他人がそのビジネス秘密を侵害したと主張する場合、その保有するビジネス秘密が法定条件に適合し、相手方当事者の情報がそのビジネス秘密と同一又は実質的に同一で、相手方当事者が不正な手段を用いた事実についての拳証責任を負わなければならない。そのうち、ビジネス秘密が法定条件に適合する証拠には、ビジネス秘密の媒体、具体的な内容、商業価値及び当該ビジネス秘密に対して講じる具体的な秘密保持措置等を含む。

そのため、企業は以下のいくつかの方面の早期警報と対応を重点的に行うべきである。

1. 早期警報制度を確立し、権利侵害行為を適時に発見する。企業は内部制度の不備や執行不利による秘密漏洩を防ぐとともに、外部からの協力や取引、侵入などの方式による漏洩にも注意を払う必要がある。秘密保持措置の効果を定期的に評価し、秘密漏洩可能なところを探し、不法取得行為、開示行為及び使用行為があるかどうかを調査し、タイムリーな警告と防備をしなければならない。

2. 一旦侵害行為が発生したら、専門チームに依頼し、適時に証拠と事実の根

拠をロックし、法律的な権利行使の考え方と方案を確定する。不法取得行為に対して、権利侵害者が権利のない又は権限を越えたビジネス秘密取得行為を実施しているかどうかを調査して証明する。開示行為に対して、指向性のある者に開示するまたは指向性のない者に開示する証拠を調査して確認する。使用行為に対して、ビジネス秘密を経営活動に投入して使用する証拠を調査して確認する。

3. 侵害状況に基づき、権利行使の方式を明確にし、対象を絞った権利行使案を選択し、当該方案が法律法規に符合していることを保証する。企業は以下の1つまたは複数の権利行使ルートを選択できる。

(1) 協議交渉：侵害者が内部侵害者、外部侵害者、または他の利益関連者に属するかを明確にし、侵害者と交渉し、ビジネス秘密漏洩が企業にもたらす損害を最大限に低減し、企業の損失を最大限に挽回する。

(2) 行政手段による権利行使：工商行政機関に申告し、行政機関と協調して意思疎通し、必要に応じて権利侵害者が企業のビジネス秘密を侵害して生産した製品の販売と使用を停止することを申請し、ビジネス秘密を侵害する関連証拠の調査と取得に協力する。

(3) 民事訴訟の賠償請求の提起：侵害者に民事訴訟を提起し、秘密漏洩者または秘密漏洩企業がビジネス秘密を侵害した証拠を収集し、判決の執行を推進する。

(4) 刑事事件を通報し、刑事手続きを推進する：公安機関に事件を通報し、公安機関の調査と証拠取得に協力し、刑事手続きを推進し、法により侵害者の刑事責任を追及する。

注意が必要なこととして、企業が最終的にどのような方法を選択して法律の保護を求めるかに関わらず、企業内部のビジネス秘密に対する保護措置を完全にし、完備することにより、提訴前の準備、有効な立証、プログラムの権利行使などの面で重要なサポートを提供することができる。