



天达共和
EAST & CONCORD

『営業秘密保護規定（2026）』 実務解説と企業コンプライアンス対応

北京天達共和弁護士事務所

管冰 弁護士

June 2026

成功，始于助人成功

Success is Rooted in Enabling Others to Achieve

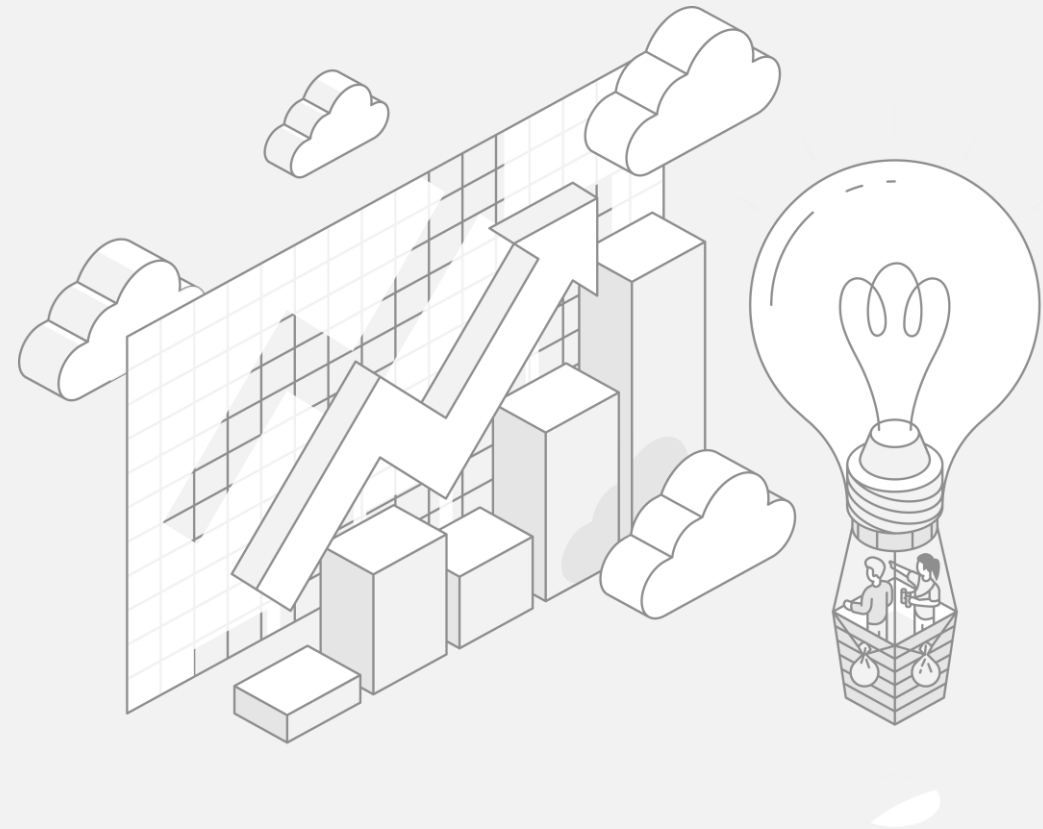
北京 / 上海 / 深圳 / 武汉 / 杭州 / 成都 / 南京 / 西安 / 广州 / 香港 / 温哥华 / 东京
Beijing / Shanghai / Shenzhen / Wuhan / Hangzhou / Chengdu / Nanjing / Xi'an / Guangzhou / Hong Kong / Vancouver / Tokyo

目次 | CONTENTS

01 制定背景と制度主旨

02 主要条項の実務的解説

03 企業コンプライアンス対応



第一部分

設定背景と制度主旨

BACKGROUND AND LEGISLATIVE INTENT

1995年旧規定の限界



制定当時の背景

- 1995年、旧国家工商行政管理局は『営業秘密侵害行為を禁止する若干規定』を公布した。
- 当時、インターネット利用は限定的であったため、営業秘密の主要媒体は紙資料・図面・顧客リスト等の物理的情報であった。



デジタル経済がもたらした実務上の課題

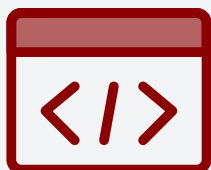
- 保護対象の「デジタル化」
- 侵害手段の「技術化」
- 権利保護メカニズムの限界



必然的な改革

- 1995年規定は条文数も限定的であり、今日のデジタル競争環境および大量データ時代に十分対応できなくなっていた。
- 今回の改正は、単なる条文追加ではなく、営業秘密保護制度全体のアップデートとして位置づけることができる。

営業秘密保護強化に向けた政策的背景



国家戦略と法整備

営業秘密保護の強化



国家レベルでの制度整備

近年、中国では営業秘密保護強化が国家戦略レベルで位置づけられている。2024年の三中全会においても、営業秘密保護制度の整備推進が明確に打ち出され、『不正競争防止法』改正の動きとも連動しながら、下位規範の整備が進められている。



総合的保護体系の形成

民事保護

損害賠償・差止請求

行政保護

市場監督管理部門による行政調査・処罰

刑事保護

重大案件に対する刑事責任追及

民事・行政・刑事が連携した総合的な保護体系を形成した。

立法目的



営業秘密保護の強化

保護範囲の拡大、認定基準の明確化、執行手段の強化を通じて、営業秘密に対する包括的な保護体制を構築する。



公正な競争秩序の維持

デジタル経済における新たな不正競争行為を明確に規制し、企業が技術革新に注力できる公正な市場環境と健全な競争秩序を確保する。



行政執行と司法実務の接続

近年の裁判実務で形成された認定ルールや立証構造を行政執行にも反映させ、営業秘密保護の実効性を高める。

第二部分

主要条項の実務的解説

IN-DEPTH INTERPRETATION OF CORE PROVISIONS AND COMPARISON

変更点1 営業秘密の定義の見直し（第5条）

要件の再構築

01

02

技術情報と経営情報
の内容の拡大

変更点 1 - ①要件の再構築(第 5 条 1 項)



非公知性

公衆に知られておらず、かつ容易に入手できない情報であること。



商業的価値 (改正ポイント)

非公知であることにより、権利者に経済的利益または競争上の優位をもたらすこと。旧規定の「実用性」よりも広い概念である。



秘密管理性

権利者が情報漏洩を防ぐために、合理的な保護措置を講じていること。

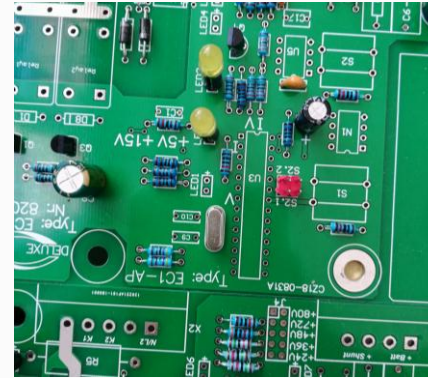
変更点 1 - ②技術情報の内容の拡大(第5条2項)



伝統的技術情報

製品開発や生産における基礎となる物理的な情報資産を指し、企業の長年の技術蓄積が反映される。

具体例：構造、原料、配合成分、材料仕様、サンプル、デザイン図面、製造工程、加工方法、生産管理方法、製品のテスト方法、品質分析方法などが含まれる。



デジタル技術情報 (改正ポイント)

デジタル経済時代の企業の中核資産である。今回の改正によって保護範囲が明確に拡大された。

具体例：業務に関する重要なデータ、アルゴリズム、コンピュータプログラム、ソースコードなどが保護対象となる。

変更点 1 - ③ 経営情報の内容の拡大(第5条3項)

01. 一般経営情報

企画・管理

事業のアイデア、内部管理方式や運用プロセスに関する情報

市場調査

業界の動向分析、顧客のニーズ調査レポート、競合分析データなどの基礎資料

計画・財務

販売目標計画、予算管理、収支予測などの戦略的な財務・事業計画情報

市場戦略

新商品の立ち上げ戦略、価格設定、プロモーション計画などの実行計画書

02. 顧客情報 (改正ポイント)



基礎属性情報

氏名（法人名）、住所、電話番号、メールアドレスなどの連絡先情報

取引習慣 (新設)

購入頻度、平均客単価、好みの製品ライン、過去の取引履歴、信用評価情報など

取引意向・内容 (新設)

交渉中の潜在案件、未公開の商談内容、将来の契約予定や共同開発の意向など

企業は顧客データベースを核心資産として厳格に管理し、取引習慣や意向情報の漏洩防止対策を強化する必要がある。

変更点2 「非公知性」認定基準の明確化（第6条）

判断時点の明確化

01

02

「整理・加工」
ルールの新設

変更点2 - ①判断時点の明確化(第6条1項)

「事後公開」は侵害の抗弁とならない

非公知性の認定

営業秘密に係る侵害が疑われる行為が発生した**時点**において、当該営業情報がその所属分野の関係者に広く知られておらず、かつ容易に入手できないこと

。

中核的解釈

侵害行為後に情報が公開されても、侵害の認定に影響しない。長年の「事後公開による抗弁」という難題がこの規定により解決された。

重要な啓示

侵害の有無は「侵害行為発生時」における秘密性に基づいて判断されるため、事後的な公開を理由とする弁解は通用しにくくなった。

変更点2 - ② 「整理・加工」ルールの新設 (第6条3項)

公開情報の独自分析・加工成果に対する保護

新規定

公開情報を整理・加工して新たに形成された情報も、非公知性を有する場合には保護対象となる。

具体例

- 公開データを独自分析した顧客分析モデル
- 公開論文を基礎として最適化したアルゴリズム
- 市場データを加工した販売予測システム

実務上の意義

企業によるデータ加工・分析活動の法的保護可能性が高まり、AI・データ活用型ビジネスへの影響も大きいと考えられる。

変更点3 「権利主体」と「秘密保持措置」の拡張

(第8-9条)

権利主体の拡大

01

02

秘密保持措置の具体化

変更点3 - ①権利主体の拡大(第8条)

ライセンサー、被授權者は独立して権利保護が可能

新規定

ライセンサーおよび授權を受けた主体についても、営業秘密の「権利者」に正式に含め、原権利者と同等の法的保護および権利行使資格を有することを明確化。

企業への影響

中国現地法人、合併会社、技術ライセンスの被許諾会社などが、迅速に対応することが可能。

変更点3 - ②秘密保持措置の具体化 (第9条)

旧規定

- NDA
- 秘密保持制度の構築
- その他合理的な秘密保持措置

VS

新規定

- 契約・人的管理
- 物理的アクセス管理
- 技術的・データ管理
- ライフサイクル管理

変更点 4 営業秘密侵害行為の類型の詳細化

(第10-14条)

- 第10条 不正取得の禁止
- 第11条 不正取得した営業秘密の開示・使用の禁止
- 第12条 秘密保持義務違反の禁止
- 第13条 教唆及び幫助の禁止
- 第14条 侵害とみなされる行為と連帯責任

変更点4 - ①営業秘密の「不正取得」の禁止(第10条)

基本原則：権利者の営業秘密を不正に取得してはならない

事業者は、**窃盗、収賄、詐欺、強迫、電子的侵入**その他の不正手段により営業秘密を取得することを禁じられている

物理的入手

書類や記憶媒体を無断で複製・占有する行為。

例：社内機密書類のスキャン、社用USBの私的持ち出し

技術的入手

システムへの不正アクセスやマルウェアを利用し、デジタル情報を盗み出す行為。

例：ID/PW窃取による不正ログイン、ウイルス感染攻撃

人的入手

従業員や関係者への金銭的買収や心理的脅迫により、情報を漏洩させる行為。

例：競合社員への賄賂提供による顧客情報の入手

不正転送

管理下にある情報を、権限のない外部場所へ移動させる行為。

例：業務データを私用クラウドへのアップロード

変更点4 - ②不正取得した営業秘密の開示・使用の禁止（第11条）

基本原則:

不正手段により取得した営業秘密については、「開示」「使用」「第三者による使用の許可」のいずれも厳しく禁止される。
取得時の違法性は、その後の利用行為全体に影響する。

⚠ 重要ポイント

営業秘密がいったん「不正取得」と評価されれば、その後に行われた利用や二次的活用も違法と判断され得る。
単に「知っていた情報を使った」だけでは免れず、情報の源流に不正があれば責任が及ぶ。

「開示」とは

権利者の許諾なく、特定の第三者や不特定多数に営業秘密を漏らす行為。

「使用」とは

情報を直接業務に利用するだけでなく、改良・修正して新製品開発に活用したり、生産工程や経営戦略の改善に利用したりする行為も含む。

🚫 典型的な違法事例

転職時に前職の製品設計図や顧客リストを持ち出し、新会社の開発や営業活動に流用する行為。

変更点4 - ③秘密保持義務違反の禁止（第12条）

適法に知り得た秘密情報であっても、守秘義務を負う

■ 義務の根拠

秘密保持義務に違反して、業務遂行上知り得た営業秘密を、第三者に開示したり、業務外で使用したり、他人の使用を許可したりしてはならない。

この義務は、単なる社内ルールに留まらず、民法や不正競争防止法に基づく法的責任を伴うため、常に厳格な遵守が求められる。

💡 重要ポイント

契約書に署名していないからといって守秘義務が免除されるわけではない。

就業規則や社会通念、業務上の信頼関係に基づき、知り得た情報は当然に守らなければならない。

■ 義務の発生源

1. 契約による明示的義務

労働契約の附則や、個別に締結する秘密保持契約（NDA）など

2. 信義誠実の原則

契約書がなくても、信頼関係に基づき当然に生じる義務

3. 業務上の明示的要求

開発・検査・委託業務等において示された守秘指示

4. 内部管理措置

就業規則や情報セキュリティ規程等に基づく遵守義務

適用対象範囲：現従業員に限らず、退職者、外部委託先、共同開発パートナー、業務提携先など、業務に関与したすべての関係者に及ぶ。

変更点4 - ④教唆及び幫助の禁止 (第13条)

禁止行為の基本原則

秘密保持義務に違反する行為を、他人に対して教唆し、誘引し、又は実行を支援することは一切禁止される。

自ら直接実行しなくても、第三者の行為を介して責任を問われ得る。

⚠ 重要な認識

「やれ」と指示したり、実行に必要な道具・情報・資金・場所を提供したりするだけでも、共同責任を問われる可能性がある。

該当する具体的な行為パターン

1. 教唆・誘引行為

明示的な指示、報酬による誘導、心理的弱みを利用した働きかけなど

2. 幫助行為

漏えい計画を知らながら、ハードウェア貸与、ソフトウェア提供、資金援助、場所の確保などを行うこと

変更点4 - ⑤侵害とみなされる行為と責任主体の拡張(第14条)

責任主体の拡大

個人、法人その他の団体が前条までの違法行為を行った場合、広く「侵害とみなされる」対象となる。

これにより、特定の事業者に限らず、さまざまな主体による不正取得・不正利用が責任追及の対象に含まれる。

🔍 法的判定における核心要素

- 情報自体の秘匿性
- 取得経路の不自然さ
- 取引価格の明らかな異常性
- 業界における通常慣行からの逸脱

第三者の責任判定

第三者が、対象情報が不法に流出したものであることを明知していた場合、又は状況から知り得たと評価される場合に、それを取得・使用・開示すると、「侵害とみなされる」可能性がある。

🚫 典型的な違法事例

元従業員から「会社のものだが、ただで譲る」と言われた顧客リストや技術資料について、その経路や背景に疑問を持たずに受け取り利用する行為。

変更点 5 行政執行手続の強化 (第16-23条)

～営業秘密侵害に対する行政救済の実効性向上～

行政取締りルートの強化

証拠収集・立証ルールの強化

行政調査権限の拡大

変更点5 - ①行政取締りルート強化（第16条～第19条）

通報から立件までのプロセスを明確化し、行政ルートの利用促進を図る

01. 行政摘発の利用を促進

- 社会による監督・通報を奨励
- 第三者からの通報も積極的に受理
- 権利者は市場監督管理局へ直接通報可能

02. 行政機関の立件基準を明文化

- 一定の要件を満たす場合、行政機関に調査開始義務が生じる
- 通報資料の具体化により、処理の予測可能性が向上する

変更点5 - ②証拠収集・立証ルールの強化(第18条、第20条、第22条)

今回の改正で最も重要な部分

侵害推定の要件

行政当局が侵害の成立を推定するための核心的要件を明確化し、被害者の立証負担を大幅に軽減した。

「実質的同一性」 + 「アクセス可能性」

権利者が営業秘密の同一性と相手方のアクセス機会を示せば、侵害が推定され、反証責任は被疑者側に移行する。



初歩的証拠の提出で手続開始可能

高度な証拠を最初から要求されず、被害者は比較的容易に行政手続を開始し、証拠保全を申請できる。



鑑定機関・専門家意見の活用を明文化

専門的知見に基づく鑑定結果や専門家意見を証拠として明確に位置付け、立証の信頼性と効率性を高めた。

変更点5 - ③行政調査権限の拡大（第21条、第23条）

01. 行政機関による調査手段の明確化

✔ 立入検査：事業所や作業場へ直接立ち入り、現場の状況を確認・記録する。

✔ 資料の閲覧・差押え：契約書、帳簿、電子データ等の閲覧・複製、及び関連物品の一時的差押えを行う。

✔ **銀行口座調査：一定の要件の下では、金融機関に対する取引状況の調査が可能となる。**

02. 一方で、行政機関にも義務が課される

☂ 調査職員に厳格な守秘義務を課す。

📄 処罰公表時には営業秘密を削除又は匿名化し、非公開とする。

変更点6 営業秘密侵害に対する行政責任の強化

(第24-26条)

～侵害行為の停止と制裁措置を明確化～

行政罰の適用
基準を明確化

侵害停止命令
の内容を具体
化

「情状が重大」
の判断基準
を明文化

変更点 6 - ①行政処罰および侵害停止措置（第24条 第25条）

01. 行政処罰の具体的な範囲

- 侵害行為の即時停止命令
- 違法に取得した営業秘密の使用禁止
- 違法所得の全額没収
- 10万～100万元の罰金
- 重大な侵害又は再犯の場合、100万～500万元の加重罰金

02. 侵害排除のための具体的措置

- 営業秘密の使用停止
- 侵害に使用した設備・技術の利用禁止
- 営業秘密資料の返還又は廃棄
- 侵害製品・半製品の廃棄処分
- 電子データの完全削除

変更点 6 - ② 「情状が重大」の判断基準を明文化（第26条）

01. 重い行政処罰の対象となるケース

権利者への深刻な影響

- 大きな経済的損害を与えた場合
- 生産・販売等の事業活動に重大な支障を及ぼした場合

公益・国家利益への侵害

- 国家利益又は公共利益を害した場合
- その他、法令上重大と評価される場合

特に注意：2年以内の再犯

過去2年以内に同種の違反行為があった再犯の場合、加重処罰が確定的になり、企業の違反履歴が直接的なリスク要因となる。

02. 実務上の意義と企業への影響

行政当局の裁量基準が明確化

- 処分適用の一貫性・予測可能性が向上
- 企業も高リスク要因を把握しやすくなる

高額罰金適用の予見可能性向上

- 「重大な情節」該当性を事前に判断しやすい
- 内部統制・従業員教育・コンプライアンス整備を促進

変更点7 域外効力 (第29条)



中国法の 「域外適用」

海外での行為でも、中国市場や権利者に実質的影響があれば適用対象となる。

海外企業・海外拠点による侵害も対象となり得る。

■ 想定されるケース

- 海外拠点から中国サーバーへの不正アクセス
- 海外企業による中国従業員への持出し誘導
- 越境データ移転時の秘密流出



企業への示唆

- 中国拠点だけでなく海外拠点も管理対象
- 本社・海外子会社を含めた統一管理が必要
- アクセス権限・データ移転・退職者管理の見直しが重要

第三部分

企業コンプライアンス対応

CORPORATE COMPLIANCE ACTION GUIDELINES

提言 1 営業秘密資産の可視化



実施すべき主要対応

- 技術情報・営業情報の洗出し
- データ資産の分類
- 営業上価値の再評価
- 機密レベル別管理



実務上の重要ポイント

従来見落とされがちであった、研究途中データ、顧客分析情報、AI学習データ等についても、営業秘密管理対象として再点検する必要がある。

提言 2 秘密管理体制の再構築

制度面

- リモートワーク規程
- BYOD管理規程
- 越境データ管理ルール

技術面

- DLP導入
- アクセス権管理
- ログ監査
- 暗号化措置

物理面

- 区域管理
- サーバー管理
- 来訪者管理



実務上の重要ポイント

秘密管理措置は、形式的に存在するだけでは不十分であり、実際に運用されていることが極めて重要である。

提言3 契約管理体系の整備

見直し対象

- 労働契約
- 秘密保持契約（NDA）
- 就業規則
- サプライヤー契約
- 共同開発契約
- 越境データ移転契約
- 退職時確認書・誓約書

実務上の重要ポイント

単なるNDA締結のみでは不十分であり、「制度・契約・運用」を一体として設計する必要がある。

提言4 侵害リスクの予防と緊急時対応体制の整備

平時対応

- アクセスログ監査
- 異常ダウンロード検知
- 退職者対応の点検
- 競合他社動向分析

有事対応

- 証拠保全手順
- 行政機関への通報フロー
- 社内調査体制
- 外部専門家連携



実務上の重要ポイント

営業秘密侵害案件では、初動対応の速度が権利保護成否を大きく左右する。

提言 5 行政的救済手段の積極活用

行政手段の特徴

- 比較的迅速な対応が可能
- 行政調査権限を活用可能
- 証拠が十分にそろわない初期段階でも対応余地がある

実務上の活用場面

- 元従業員転職案件
- データ持出し案件
- サプライチェーン流出案件



実務上の重要ポイント

民事訴訟・刑事対応と組み合わせた複合的戦略が、今後より重要となる。

提言 6 「適法取得」の抗弁に留意する

目 実施すべき主要対応

- 新規採用時の確認 前職の営業秘密を持ち込まないことの確認
- 開発記録整備 研究開発過程の文書化
- ソース管理 開発履歴・変更履歴保存
- 外部技術導入審査 技術来源の適法性確認

盾 実務上の重要ポイント

今後は、「侵害していないこと」を企業側が日常的に立証可能な状態にしておくことが重要となる。

結語 営業秘密保護を「経営課題」として再定義する



課題

デジタル化・越境化が進む中、企業に求められる秘密管理水準は確実に高度化している。



機会

一方で、行政執行・立証ルールの整備により、企業の権利保護手段も実務上大きく強化された。



行動

営業秘密保護を法務部門のみの問題としてではなく、経営・人事・IT・事業部門を含む全社的ガバナンスとして再構築する必要がある。



目標

自社の技術・データ・顧客情報といった中核資産を、持続的な競争優位につなげること。

営業秘密保護は、単なる「防御法務」ではなく、企業競争力そのものを支える経営戦略課題へと変化している。

Q & A

ご清聴ありがとうございました。

THANKS FOR LISTENING