TMI 総合法律事務所
中 国 最 新 法 令 情 報

－2025 年 10 月号－

皆様には、日頃より弊事務所へのご厚情を賜り誠にありがとうございます。

お客様の中国ビジネスのご参考までに、「中国最新法令情報」をお届けします。記事の内容やテーマについてご要望やご質問がございましたら、ご遠慮なく弊事務所へご連絡下さい。

― 目 次 ―

◆ 本ニュースレターの内容は、一般的な情報提供であり、個別の案件に適用可能な具体的な法的アドバイスを含むものではありません。

◆ ニュースレターの配信停止をご希望の場合には、本ニュースレター末尾記載の連絡先までご連絡をいただきますようお願い致します。

I. 最新法令情報（2025 年 9 月中旬～2025 年 10 月中旬）

◆ 企業が競業避止義務を実施するためのコンプライアンスガイダンス[1]

人力資源社会保障部　2025 年 9 月 4 日公布　2025 年 9 月 4 日施行

1. はじめに

2025 年 9 月 4 日、人力資源社会保障部は「企業が競業避止義務を実施するためのコンプライアンスガイダンス」（以下「**ガイダンス**」という。）を発表し、企業が参照の上実施するよう供するとともに、各地の人力資源社会保障部門に対し、企業が競業避止義務の範囲を科学的に界定し、実施プロセスを規範化し、労働者と公平に関連する権利義務を合意し、企業の営業秘密と労働者の就業・職業選択の権利の双方を保護するよう指導することを求めた。

競業避止義務とは、企業が営業秘密保持義務を負う労働者と合意し、労働契約の解除または終了後一定期間、労働者が自社と同一または類似の製品の生産・経営、同一または類似の業務に従事する競争関係にある他の企業に就職すること、または自ら同一または類似の製品の生産・経営、業務に従事する事業を開業することを禁止することをいう[2]。

近年、一部企業において、恣意的に競業避止義務の範囲を拡大する現象が見られ、労働者の就業・職業選択の権利が十分に保護されていない状況があった。企業の営業秘密を保護するとともに、労働者の正当な権利利益を実質的に維持するため、ガイダンスは、「最高人民法院による労働紛争事件の審理における法律適用問題に関する解釈（二）」の関連規定に基づき、競業避止義務の具体的内容をさらに細分化し、企業のコンプライアンス対応にとって重要な指導的意義を有する。

2. 要点

（1）競業避止義務の適用対象

競業避止義務の適用対象は、労働関係を構築し、営業秘密保持義務を負う労働者である[3]。例えば、企業は、営業秘密を知り得る管理職、上級技術者その他秘密保持義務を負う者と競業避止契約を締結することができる[4]。業界で通用する専門知識及び技能のみを掌握し、業務で接触する情報が企業の一般的な経営情報に限られる労働者は、秘密保持義務を負う者に該当しないため[5]、企業は当該労働者と競業避止契約を締結することはできない。

（2）競業避止義務の適用客体

競業避止義務の適用客体である営業秘密は、秘密性、価値性及び保密性を備えなければならない。ガイダンスは、営業秘密の定義と範囲、すなわち公衆に知られておらず、商業的価値を有し、かつ企業が相応の保密措置を講じた技術情報、経営情報等の商業情報であることを明確にしている[6]。業界における一般常識または業界慣行であり、公開された経路から入手可能な商業情報は、営業秘密に該当しない[7]。

---

[1]「企业实施竞业限制合规指引」
[2] ガイダンス第 3 条
[3] ガイダンス第 2 条
[4] ガイダンス第 7 条第 1 項
[5] ガイダンス第 7 条第 3 項
[6] ガイダンス第 4 条第 1 項
[7] ガイダンス第 4 条第 2 項

労働者と競業避止義務を合意するにあたり、企業はまず保有する営業秘密の内容と範囲を確認し[8]、優先的に営業秘密保護措置を講じる必要がある[9]。

（3）競業避止義務の適用基準

ア　合理的かつ必要な原則及び信義誠実の原則に従うこと

a. 競業避止義務の後置

企業は、必要かつ合理的な原則に従い、営業秘密の知悉権限の管理、営業秘密データの暗号化、合理的な脱密期間の設定等の営業秘密保護措置を優先的に講じ、競業避止義務者の範囲、就業を制限する企業及び地域等を恣意的に拡大してはならない[10]。

b. 必要性評価の実施

企業が競業避止義務を実施することを決定した場合、必要性評価を実施しなければならず、企業の営業秘密を知悉もしくは接触していない労働者を競業避止義務の範囲に含めてはならない[11]。評価過程では評価記録を保存する必要があり、ガイダンスは評価の具体的な手続きを規定していないが、企業は独自に評価基準とプロセスを定めることができる。

c. 就業制限の範囲及び地域の合理的な合意

労働者と合意する就業制限の範囲及び地域については、企業は、経営範囲、商業競争の状況及び労働者の営業秘密の知悉状況等に基づき、合理的に合意しなければならない[12]。

就業制限の範囲については、自社と同一または類似の製品の生産・経営、同一または類似の業務に従事する競争関係にある他の企業に限定すべきである。また、可能な限り就業制限する企業の範囲について具体的かつ明確な合意を行い、条件が整えば競業避止義務対象企業リストを列記することができる[13]。

就業制限の地域については、企業の経営業務の範囲と合致すべきであり、十分な理由なく全国または全世界としてはならない。範囲を全国または全世界とする場合は、契約においてその理由を十分に説明する必要がある[14]。

d. 信義誠実の原則の遵守

企業は、合法的かつ誠実に労働者と競業避止契約を締結し、双方の権利義務を公平に合意しなければならず、優越的な地位を利用して労働者に違法または著しく公平性を欠く条項の受諾を強制してはならない[15]。

イ　事前告知

営業秘密を知り得る管理職、上級技術者以外のその他秘密保持義務を負う者に対して競業避止義務を合意する場合は、事前にその理由を告知し、保持すべき営業秘密の具体的な内容を説明しな

[8] ガイダンス第５条
[9] ガイダンス第６条
[10] ガイダンス第６条第１項
[11] ガイダンス第６条第２項
[12] ガイダンス第10条第１項
[13] ガイダンス第10条第２項
[14] ガイダンス第10条第３項
[15] ガイダンス第10条

ければならない[16]。

ウ　就業規則は競業避止合意に代えることができない

企業は、法定に基づき作成した就業規則において、労働者の秘密保持義務の履行、保密制度、保密措置及び競業避止義務の実施原則、対象となる職務、就業制限の範囲、経済的補償の基準等について一般的な規定を設けることはできるが、就業規則をもって競業避止合意に代えることはできない[17]。競業避止合意は、就業規則に基づき、かつ労働契約、秘密保持契約または競業避止契約中に明確に記載されなければならない[18]。

エ　競業避止義務の期間

競業避止義務の期間は、労働者の秘密関与の程度及び営業秘密の時効性に基づき合理的に定め、最長で２年を超えてはならない[19]。

3. 競業避止義務の補償金及び違約金

（1）競業避止義務の補償金

ガイダンス第 12 条は、企業が労働者に競業避止義務の履行を求める場合、経済的補償を支払わなければならないと規定する。具体的な要求は以下を含む：
営業秘密の研究開発コスト及び商業的価値、就業制限の範囲、労働者の在職期間中の賃金水準、労働者の就業・職業選択及びキャリア発展への影響等、総合的な要素を考慮して合理的に決定する必要がある[20]。

月額の経済的補償は、一般的に、労働契約の解除または終了前 12 ヶ月の労働者の平均賃金の30%を下回らず、かつ労働契約履行地の最低賃金基準を下回ってはならない。競業避止義務の期間が 1 年を超える場合、月額の経済的補償は、一般的に、労働契約の解除または終了前 12 ヶ月の労働者の平均賃金の 50%を下回らないものとする[21]。

労働契約の解除または終了後、企業は競業避止義務の期間中、金銭の形で毎月労働者に競業避止義務の経済的補償を遅滞なく支払わなければならず、日常的に労働者に支給する賃金・賞与に既に競業避止補償が含まれていることを理由に支払いを拒否してはならない[22]。合意に従い競業避止義務の期間中に経済的補償を支給しなかった企業に対して、労働者は人力資源社会保障行政部門にクレームを申し出ることができる[23]。

（2）競業避止義務の違約金

企業は、労働者と競業避止義務違反による違約金を合意することができる。違約金の額は、労働者が営業秘密を漏洩した場合に生じうる経済的損失、企業が労働者に支払う競業避止義務の経済的補償の額に基づき合理的に決定し、一般的に合意した競業避止義務の経済的補償総額の 5 倍を超えないものとする[24]。

---

[16] ガイダンス第７条第２項
[17] ガイダンス第８条第１項
[18] ガイダンス第９条第１項
[19] ガイダンス第 11 条
[20] ガイダンス第 12 条第２項
[21] ガイダンス第 13 条
[22] ガイダンス第 16 条
[23] ガイダンス第 21 条
[24] ガイダンス第 14 条

労働者が競業避止義務の合意に違反し、または各種の方法により競業避止義務の合意を回避した場合、企業は労働者に対し、合意に従い違約金の支払いを求め、かつ労働者に競業避止義務の履行継続を求めることができる。労働者が違約金の支払いを拒否した場合、企業は法に基づき仲裁の申請、訴訟の提起をすることができる。労働者が競業避止義務の合意に違反し、企業が被った損失が違約金の基準を超える場合、企業は関連当事者に対し損害賠償責任の負担を求めることができる[25]。

◆ サイバーセキュリティ事件報告管理弁法[26]

国家インターネット情報弁公室　2025 年 9 月 11 日公布　2025 年 11 月 1 日施行

1. はじめに

2025 年 9 月 11 日、国家インターネット情報弁公室は「国家サイバーセキュリティ事件報告管理弁法」（以下「**報告管理弁法**」という。）を公布し、2025 年 11 月 1 日より施行される。サイバーセキュリティ事件の報告管理を規範化し、サイバーセキュリティ事件による損失と危害を速やかに制御するため、報告管理弁法は、サイバーセキュリティ事件報告の要件をさらに細分化した。中国域内においてネットワークを建設・運営し、またはネットワークを通じてサービスを提供するネットワーク運営者[27]は、サイバーセキュリティ事件が発生した場合、報告管理弁法の規定に従って報告しなければならない。

2. 要点

（1） サイバーセキュリティ事件の分類

報告管理弁法においてサイバーセキュリティ事件とは、人為的原因、ネットワークへの攻撃、ネットワークに存在する脆弱性や潜在リスク、ソフトウェア・ハードウェアの欠陥または故障、不可抗力等の要因により、ネットワーク及び情報システムまたはその中のデータ・業務アプリケーションに危害が生じ、国家、社会、経済に悪影響を及ぼす事件を指す[28]。

報告管理弁法は、別紙として付された「サイバーセキュリティ事件分類ガイドライン」によりサイバーセキュリティ事件を分類し、事件の深刻度及び影響に基づき、特に重大なサイバーセキュリティ事件、重大なサイバーセキュリティ事件、やや重大なサイバーセキュリティ事件及び通常のサイバーセキュリティ事件の四つのカテゴリーに区分している。

サイバーセキュリティ事件	状況	
	合致	判断
特に重大なサイバーセキュリティ事件	以下のいずれかの状況に該当するものは、特に重大なサイバーセキュリティ事件とする。 1. 重要ネットワーク及び情報システムが特に深刻なシステム損害を受け、	通常、以下の条件のいずれかを満たす場合、特に重大なサイバーセキュリティ事件と判断できる。 1. 省クラス以上の党政機関のポータルサイト、中央重点ニュースサイトが、攻撃・故障により、24 時間以上アクセス不能となった。

[25] ガイダンス第 19 条第 2 項、第 3 項
[26]「国家网络安全事件报告管理办法」
[27] 報告管理弁法第 12 条第 2 項に基づき、ネットワーク運営者とは、ネットワークの所有者、管理者及びネットワークサービス提供者を指す。
[28] 報告管理弁法第 12 条第 1 項

サイバーセキュリティ事件	状況	
	合致	判断
	システムが広範囲に麻痺し、業務処理能力を喪失した。 2. 核心データ、重要データ、大量の個人情報が消失、窃取、改ざん、なりすましの対象となり、国家安全保障と社会の安定に対して特に深刻な脅威をもたらした。 3. その他、国家安全保障、社会秩序、経済建設及び公衆の利益に対して特に深刻な脅威をもたらし、特に深刻な影響を及ぼしたサイバーセキュリティ事件。	2. 重要情報インフラストラクチャーが全体として6時間以上中断、または主要機能が24時間以上中断した。 3. 一つまたは複数の省クラス行政区域の人口の50%以上、または1000万人以上において、水道、電力、ガス、石油、暖房、交通、通院、買い物等の仕事・生活に影響が生じた。 4. 核心データ、重要データが漏えい、窃取、改ざん、なりすましの対象となり、国家安全保障と社会の安定に対して特に深刻な脅威をもたらした。 5. 1億人以上の個人情報が漏えいした。 6. 省クラス以上の党政機関のポータルサイト、中央重点ニュースサイト、超大規模ネットワークプラットフォーム等が攻撃により改ざんされ、違法有害情報が特大範囲で拡散した。以下のいずれかの状況をもって「特大範囲」と認める。 (1) ホームページに表示され6時間以上持続した、または他のページに表示され24時間以上持続した。 (2) ソーシャルプラットフォームで10万回以上転載された。 (3) 閲覧またはクリック数が100万以上であった。 (4) 省クラス以上のネットワーク情報部門、公安機関が「特大範囲での拡散」と認定した。 7. 1億元以上の直接的経済的損失を生じさせた。 8. その他、国家安全保障、社会秩序、経済建設及び公衆の利益に対して特に深刻な脅威をもたらし、特に深刻な影響を及ぼしたサイバーセキュリティ事件。
重大なサイバーセキュリティ事件	以下のいずれかの状況に該当し、かつ特に重大なサイバーセキュリティ事件に該当しないものは、重大なサイバーセキュリティ事件とする。 1. 重要ネットワーク及び情報システムが深刻なシステム損害を受け、システムが長時間中断または一部麻痺し、業務処理能力が大きく影響を受けた。 2. 核心データ、重要データ、多量の個人情報が消失、窃取、改ざん、なりすましの対象となり、国家安全保障と社会の安定に対して深刻な脅威をもたらした。 3. その他、国家安全保障、社会秩序、経済建設及び公衆の利益に対して深刻な脅威をもたらし、深刻な影響を及ぼしたサイバーセキュリティ事件。	通常、以下の条件のいずれかを満たす場合、重大なサイバーセキュリティ事件と判断できる。 1. 地区市クラス以上の党政機関、企業・事業単位のポータルサイト、省クラス以上の重点ニュースサイトが、攻撃・故障により、6時間以上アクセス不能となった。 2. 重要情報インフラストラクチャーが全体として1時間以上中断、または主要機能が3時間以上中断した。 3. 一つまたは複数の地区市クラス行政区域の人口の50%以上、または100万人以上において、水道、電力、ガス、石油、暖房、交通、通院、買い物等の仕事・生活に影響が生じた。 4. 核心データ、重要データが漏えい、窃取、改ざん、なりすましの対象となり、国家安全保障と社会の安定に対して深刻な脅威をもたらした。 5. 1000万人以上の個人情報が漏えいした。 6. 地区市クラス以上の党政機関、企業・事業単位のポータルサイト、省クラス以上の重点ニュースサイト、大規模以上のネットワークプラットフォーム等が攻撃により改ざんされ、違法有害情報が広範囲で拡散した。以下のいずれかの状況をもって「広範囲」と認める。

サイバーセキュリティ事件	状況	
	合致	判断
		(1) ホームページに表示され 2 時間以上持続した、または他のページに表示され 12 時間以上持続した。 (2) ソーシャルプラットフォームで 1 万回以上転載された。 (3) 閲覧またはクリック数が 10 万以上であった。 (4) 省クラス以上のネットワーク情報部門、公安機関が「広範囲での拡散」と認定した。 7. 2000 万元以上の直接的経済的損失を生じさせた。 8. その他、国家安全保障、社会秩序、経済建設及び公衆の利益に対して深刻な脅威をもたらし、深刻な影響を及ぼしたサイバーセキュリティ事件。
やや重大なサイバーセキュリティ事件	以下のいずれかの状況に該当し、かつ重大なサイバーセキュリティ事件に該当しないものは、やや重大なサイバーセキュリティ事件とする。 1. 重要ネットワーク及び情報システムがやや大きなシステム損害を受け、システムが中断し、システム効率が明らかに影響を受け、業務処理能力が影響を受けた。 2. 重要データ、やや多量の個人情報が消失、窃取、改ざん、なりすましの対象となり、国家安全保障と社会の安定に対してやや深刻な脅威をもたらした。 3. その他、国家安全保障、社会秩序、経済建設及び公衆の利益に対してやや深刻な脅威をもたらし、やや深刻な影響を及ぼしたサイバーセキュリティ事件。	通常、以下の条件のいずれかを満たす場合、やや重大なサイバーセキュリティ事件と判断できる。 1. 地区市クラス以上の党政機関、企業・事業単位のポータルサイト、省クラス以上の重点ニュースサイトが、攻撃・故障により、2 時間以上アクセス不能となった。 2. 重要情報インフラストラクチャーが全体として 10 分以上中断、または主要機能が 30 分以上中断した。 3. 一つまたは複数の地区市クラス行政区域の人口の 30%以上、または 10 万人以上において、水道、電力、ガス、石油、暖房、交通、通院、買い物等の仕事・生活に影響が生じた。 4. 重要データが漏えい、窃取の対象となり、国家安全保障と社会の安定に対してやや深刻な脅威をもたらした。 5. 100 万人以上の個人情報が漏えいした。 6. 党政機関、企業・事業単位のポータルサイト、重点ニュースサイト、ネットワークプラットフォーム等が攻撃により改ざんされ、違法有害情報がやや広い範囲で拡散した。以下のいずれかの状況をもって「やや広い範囲」と認める。 (1) ホームページに表示され 30 分以上持続した、または他のページに表示され 2 時間以上持続した。 (2) ソーシャルプラットフォームで 1000 回以上転載された。 (3) 閲覧またはクリック数が 1 万以上であった。 (4) 省クラス以上のネットワーク情報部門、公安機関が「やや広い範囲での拡散」と認定した。 7. 500 万元以上の直接的経済的損失を生じさせた。 8. その他、国家安全保障、社会秩序、経済建設及び公衆の利益に対してやや深刻な脅威をもたらし、やや深刻な影響を及ぼしたサイバーセキュリティ事件。
通常のサイバーセキュリティ事件	上記のサイバーセキュリティ事件以外で、国家安全保障、社会秩序、経済建設及び公衆の利益に対して一定の脅威をもたらし、一定の影響を及ぼしたサイバーセキュリティ事件。	

（2） ネットワーク運営者の報告手続き

ネットワーク運営者は、自単位に関わるサイバーセキュリティ事件を発見または認知した場合、上記「サイバーセキュリティ事件分類ガイドライン」の規定に従って判断し、やや重大以上のサイバーセキュリティ事件に該当する場合は、以下の手続きに従って報告しなければならない[29]。

報告主体	サイバーセキュリティ事件	報告/通知対象	時間制約
ネットワーク運営者	やや重大以上のサイバーセキュリティ事件で、かつ重要情報インフラに関わるもの	保護作業部門、公安機関	第一報を速やかに報告、遅くとも 1 時間以内
保護作業部門	重大、特に重大なサイバーセキュリティ事件	国家ネットワーク情報部門、国務院公安部門	ネットワーク運営者からの報告受領後速やかに報告、遅くとも 30 分以内
中央・国家機関各部委及びその直轄単位のネットワーク運営者	やや重大以上のサイバーセキュリティ事件	当該部門のネットワーク情報工作機構	速やかに報告、遅くとも 2 時間以内
各部門のネットワーク情報工作機構	重大、特に重大なサイバーセキュリティ事件	国家ネットワーク情報部門	報告受領後速やかに報告、遅くとも 1 時間以内
国家ネットワーク情報部門	重大、特に重大なサイバーセキュリティ事件	関係部門への通知	報告受領後速やかに通知
その他のネットワーク運営者	やや重大以上のサイバーセキュリティ事件	属地の省クラスネットワーク情報部門	速やかに報告、遅くとも 4 時間以内
省クラスネットワーク情報部門	重大、特に重大なサイバーセキュリティ事件	国家ネットワーク情報部門への報告、同時に同級の関係部門への通知	報告受領後速やかに報告、遅くとも 1 時間以内
ネットワーク運営者	犯罪の嫌疑がある場合	公安機関	速やかに届出

（3）サイバーセキュリティ事件の報告内容

サイバーセキュリティ事件を報告する際には、以下の内容を含むものとする。規定時間内に事件の原因、影響または発展傾向等を判断できないサイバーセキュリティ事件については、まず①号、②号の内容を報告し、その他の状況は速やかに追加報告することができる。サイバーセキュリティ事件を報告した後、新たに重要な状況が生じた場合、または調査作業が段階的な進展を得た場合、当事者単位は速やかに報告しなければならない[30]。

① 当事者単位の名称及び当事者システムまたは施設の基本状況
② サイバーセキュリティ事件を発見または発生した時間、場所、類型、レベル、及び既に生じた影響と危害、既に講じた措置及びその効果。ランサムウェア攻撃事件については、さらに支払いを要求する身代金の金額、方法、期日等を含む。
③ 事件の状況の発展傾向及びさらなる影響と危害の可能性
④ サイバーセキュリティ事件の原因に関する予備的分析意見
⑤ 原因追跡調査の手がかり。考え得る攻撃者情報、攻撃経路、存在する脆弱性等を含むがこれらに限らない。
⑥ 今後講じる予定の対応措置及び支援要請事項

[29] 報告管理弁法第 4 条
[30] 報告管理弁法第 7 条

⑦　サイバーセキュリティ事件現場の保護状況
⑧　その他報告すべき状況

（4）サイバーセキュリティ事件処置後のフォローアップ作業

サイバーセキュリティ事件の処置作業が終了した後、ネットワーク運営者は、30 日以内に、関連事件の発生原因、緊急対応措置、生じた危害、責任追及、改善是正状況、教訓等について全面的に分析・総括し、事件処置総括報告書を作成の上、元の報告経路を通じて上報しなければならない[31]。

（5）法的責任

報告管理弁法第 10 条は、ネットワーク運営者が報告管理弁法の規定に従ってサイバーセキュリティ事件を報告しなかった場合の罰則を規定するが、処罰の軽重の程度のみを規定し、具体的な処罰措置については、所管の主管部門が関係法律、行政法規の規定に従って処罰を行うものとする。ここで関係する法律・法規には、「サイバーセキュリティ法」、「データセキュリティ法」、「個人情報保護法」、「重要情報インフラ安全保護条例」等が含まれる可能性がある。

報告管理弁法第 11 条は、サイバーセキュリティ事件が発生した際、ネットワーク運営者が合理的かつ必要な防護措置を既に講じ、応急予案に従って処置を行い、サイバーセキュリティ事件の影響と危害を効果的に低減させ、かつ報告管理弁法の規定に従って速やかに報告した場合、情状により当該単位及び人員の責任を軽減または不問とすることができると規定している。

◆ 電子印章管理弁法[32]

国務院事務局　2025 年 10 月 9 日公布　2025 年 10 月 9 日施行

1. はじめに

2025 年 10 月 9 日、国務院事務局は「電子印章管理弁法」（以下「**管理弁法**」という。）を公布し、同日、施行された。デジタル化が進展する現代において、管理弁法を通じて電子印章の規範的な管理を強化し、電子印章の普遍的応用を推進することが期待される。

2. 要点

（1）適用範囲

管理弁法は、行政機関、企業・事業単位、社会組織その他法定に基づき設立された組織（以下、総称して「**単位（組織）**」という。）の法定名称章、法定名称を冠した内部機構章、支社・支店章、業務専用章、並びに単位（組織）の事務処理に用いられる個人名章等の電子印章の管理及び応用活動に適用される[33]。

電子印章とは、管理弁法第 2 条の規定によれば、暗号技術及び関連するデジタル技術に基づき印章を表征する特定の形式のデータを指し、電子文書に対する信頼性のある電子署名を実現するために用いられる。電子印章は、印章画像データ、印章名称、印章所有者情報、電子署名認証証明書及びそれに関連する電子署名作成データ等を含む。このことから、電子印章は単なる印章の画

[31] 報告管理弁法第 8 条
[32]「电子印章管理办法」
[33] 管理弁法第 3 条

像ではなく、特定の形式のデータであることが分かる。

管理弁法の規定に適合する電子印章は、実物の印章と同等の法的効力を有する[34]。契約締結時などに電子印章を選択して利用することができ、この効力の同一性は、デジタル化が進んだ現代において電子印章の適用性を広く高め、利便性をさらに向上させている。

（2）管理及びサービス主体

電子印章の管理及びサービス主体には、国家レベルでは国家暗号管理局、国務院事務局、工業情報化部及び公安機関が含まれ、主に電子印章の管理、電子印章の相互信頼・相互承認の推進、監督管理及び普及推進等を担当する[35]。地方及び部門レベルでは、電子印章の管理単位を明確にし、電子印章の作成、届出及び管理を行うことが求められる[36]。

（3）電子印章の作成等に関する要求及びプロセス

ア　提出を要する書類・情報

管理弁法第 14 条に基づき、単位（組織）は要求に従い、真実、適法かつ有効な作成材料を提出し、電子印章作成管理単位による照合を受けなければならない。関連する材料は以下を含む。

① 電子印章申請が承認されたことを証明する関連書類
② 単位（組織）の設立承認文書または設立登記証明書
③ 電子印章を作成するための関連データ及び情報
④ 電子印章作成管理単位が提出を規定するその他の資料

イ　作成に関する要求

電子印章の作成に関する要求は、以下の通りである[37]。

① 電子印章の電子署名認証証明書は、適法かつ有効であり、法令に基づき設立された電子政務電子認証サービス機構または電子認証サービス機構により発行されなければならず、電子印章の有効期限の満了日時は、電子印章所有者[38]の電子署名認証証明書の有効期限の満了日時を超えてはならない。
② 電子印章のデータ形式、生成プロセス及び応用インターフェースは、国家の関連する標準規範に適合しなければならない。
③ 電子印章の画像仕様、様式等の画像データは、印章管理に関する法律・法規において明確にされた印影の規制と一致しなければならず、必要に応じて電子印章関連の表示文言を付加することができる。対応する実物印章が存在しない場合、電子印章の画像データは類似の実物印章の印影規制を参照することができる。

ウ　届出

電子印章の作成完了後、電子印章作成管理単位が直接届出を行うため、単位（組織）が別途届出

[34] 管理弁法第 5 条
[35] 管理弁法第 6 条～第 9 条
[36] 管理弁法第 10 条、第 11 条
[37] 管理弁法第 16 条
[38] 管理弁法第 34 条第 1 号に基づき、電子印章所有者とは、電子印章に対する所有権を有する単位（組織）または個人を指す。電子印章の電子署名作成データは、電子印章所有者が専有する。

する必要はない。ただし、電子印章の使用停止、復旧等の状態変更が生じた場合、電子印章所有者または関連単位は、速やかに電子印章作成管理単位に対して届出を行わなければならない[39]。届出後は、電子印章作成管理単位において情報照会を行うことができる[40]。

エ　再作成

電子印章に以下のような状況が生じた場合、電子印章所有者は電子印章作成管理単位に対して再作成を申請しなければならない[41]。

- 電子印章の有効期限が満了した場合
- 電子印章の媒体が損傷または紛失した場合
- 電子署名作成データが逸失した場合

オ　登録抹消

電子印章に以下のような状況が生じた場合、電子印章所有者は要求に従い、速やかに電子印章発行部門に対して電子印章の登録抹消を申請しなければならず、電子印章作成管理単位は、電子印章発行部門の処理意見に基づき、登録抹消が必要な電子印章について登録抹消の手続きを行う[42]。

- 名称変更
- 解散
- 撤廃
- 営業許可等の取消し
- 破産
- 分割
- 合併

電子印章に登録抹消すべき状況が存在するにもかかわらず、電子印章所有者が登録抹消を申請しない場合、または速やかに申請できない場合、電子印章発行部門が登録抹消の処理意見を提出し、電子印章作成管理単位において、登録抹消が必要な電子印章について登録抹消の手続きを行う[43]。

（4）電子印章に対する管理責任

電子印章の使用管理は、「所有する者がこれを管理し、調印し、責任を負う」の原則に従う[44]。電子印章所有者は、管理の全過程において、完善された情報保護制度を確立し、電子印章関連情報の安全を確保するために必要な措置を講じ、収集した単位（組織）及び個人の情報を厳重に保密し、未承認のアクセス及び情報の漏洩、改ざん、毀損、紛失を防止しなければならない[45]。

電子印章管理の職責は電子印章所有者に帰属し、電子調印[46]データの真実性、完全性及び否認防止性を保証し、かつ電子署名過程の情報を記録及び保存しなければならない[47]。

---

[39] 管理弁法第 17 条第 1 項
[40] 管理弁法第 17 条第 2 項
[41] 管理弁法第 18 条
[42] 管理弁法第 19 条第 1 項
[43] 管理弁法第 19 条第 2 項
[44] 管理弁法第 21 条
[45] 管理弁法第 28 条
[46] 管理弁法第 34 条第 2 項に基づき、電子調印とは、電子印章を使用して電子文書に署名する過程を指し、これによって形成される結果データが電子調印データである。
[47] 管理弁法第 22 条

注意すべき点は、電子調印を行う際には、電子調印データの真実性、完全性及び否認防止性を検証し、かつ電子調印時点における電子印章の有効性を検証し[48]、電子印章の無効に起因する損失を回避しなければならないことである。さらに、電子調印がなされた電子文書を保存する場合、電子記録管理に関する関連規定及び標準規範にも適合しなければならない[49]。

管理が不適切な電子印章所有者は、法令に基づき法的責任を負担するリスクが存在する[50]。

執筆担当：申 含章

[48] 管理弁法第 23 条
[49] 管理弁法第 24 条
[50] 管理弁法第 32 条

II. 中国法務の現場より

◆ 中国データ実務におけるセンシティブ個人情報への関心の高まり

中国の個人情報保護法（以下「**法**」という。）が施行されてから、まもなく 4 年が経過する。この間、国家インターネット情報弁公室（CAC）をはじめとする当局から数多くのガイドラインや補助規範が相次いで公表され、企業のデータガバナンス実務も徐々に成熟してきた。施行当初こそ、欧州の GDPR に類似しながらもところどころで中国特有の制度設計が施された法律に戸惑う企業も見られたが、現在では社内の体制整備やデータ移転プロセスの運用を通じて、一定の安定期を迎えつつあるように思われる。

私も日本企業クライアントの国際的なデータガバナンス体制をご支援する立場で様々な事例を見てきたが、中国の実務において特に重要なキーワードの一つが「センシティブ個人情報」かと思う。中国の個人情報保護法第 28 条は、センシティブ個人情報を次のように定義している。「センシティブ個人情報とは、ひとたび漏えいし、または不法に使用されると、自然人の人格的尊厳が侵害を受け、または人身もしくは財産的な安全に危害を与えやすい個人情報を指し、生体認証、宗教に関する信仰、特定の身分、医療健康、金融口座及び移動履歴等の情報並びに 14 歳未満の未成年者の情報が含まれる。」

この「センシティブ個人情報」概念が実務上大きな注目を集めるきっかけとなったのが、2024 年 3 月に公表された「データの越境流動促進と規範規定」である。この規定の背景として、法第 38 条第 1 項は、個人情報の越境移転を行う場合に、(i)データ越境移転影響評価を受ける、(ii)第三者機関による個人情報保護認証を受ける、または(iii)移転元と移転先との間で標準契約を締結する、のいずれかの手続きを求めている。このうち、事業者にとって最も利用しやすいのは(iii)の標準契約であったが、2023 年に施行された「個人情報越境移転標準契約弁法」により、締結後の当局届出が義務化され、実務上の負担が一段と増した。こうした背景のもと、本規定では、一定の条件を満たす場合に限り、標準契約の締結及び当局届出を免除するという重要な緩和措置が導入された。

この免除要件の中でも特に注目を集めたのが、「当年 1 月 1 日から起算して、中国国外に越境移転した個人情報（センシティブ個人情報を除く）が 10 万人未満であること」という条件である。「センシティブ個人情報を除く」という括弧書きがあるので、越境移転の対象となるデータの中にセンシティブ個人情報が一部でも含まれていれば、この免除の適用を受けることができない。この点が、日系企業のデータ管理実務に大きな影響を与えた。実際に、日本本社から中国子会社データへのアクセス権限の設定を見直し、センシティブ個人情報が含まれないよう情報区分を再設計した企業も見られる。結果として、センシティブ個人情報をいかに特定し、可能な限り越境移転を避けるかが、法令対応上の重要テーマとなっている。こうした意味で、中国法における「センシティブ個人情報」という概念は、他国法以上に実務的な重みをもっているといえる。

もっとも、センシティブ個人情報の定義は必ずしも明確ではない。法第 28 条は具体例を挙げているが、これらに限定されるわけではなく、「漏えいまたは不法に使用されることによって、個人の尊厳や身体・財産の安全に影響を及ぼしうる情報」が該当する。そのため、何がセンシティブ個人情報にあたるのかを判断するには、「センシティブ個人情報識別ガイドライン」や国家標準である「情報安全技術 個人情報安全規範（GB/T 35273-2020）」を参照することが有益である。これらは実質的に、企業が内部方針を策定する際の判断基準として活用されている。

さらに、センシティブ個人情報の取扱いに関して忘れられがちなのが、個人情報保護影響評価（PIA）の実施義務である。中国で「影響評価」というと、越境移転時に必要となる越境移転影響評価」（法 55 条第 4 項）を想起しがちだが、センシティブ個人情報を取扱う場合にも影響評価が求められている（法 55 条第 1 項）。影響評価においては、取扱目的の正当性、必要性、リスク対策などを文書化し、結果を記録・保存することが義務付けられており、社内管理手続の一環として軽視できない。

中国のデータ規制は、越境データ移転の緩和という方向に舵を切りつつも、その実務運用は「センシティブ個人情報」を境界として厳格さを維持している。中国のデータ管理をめぐる実務方針としては、まず自社データの中でセンシティブ個人情報に該当しうる項目を特定し、必要に応じてデータ取得を見直したり、データ区分やアクセス権限を再設計すること、それに必要に応じて影響評価を実施したうえで記録化していくことが、コンプライアンス確保の第一歩となる。

執筆担当：杉浦　翔太

III. バックナンバー

過去 1 年間の中国最新法令情報のバックナンバーは以下のとおりです。
号数をクリックいただきますとブラウザ上で閲覧ができますので、ご参照ください。

号数	紹介法令/判例	今月の中国関連ブログ記事／連載・コラム
2025 年 9 月号	• 会社登記強制抹消制度実施弁法 • 仲裁法（2025 年改正） • 企業破産法改正案（意見募集稿）	• 中国商標審査の最新状況
2025 年 8 月号	• 最高人民法院による労働紛争事件の審理における法律適用問題に関する解釈（二） • ネットワーク情報部門による行政処罰裁量権基準の適用に関する規定 • サイバーセキュリティ標準実践ガイドラインにおける QR コード注文に関する個人情報保護要求（意見募集稿）	• 労働紛争に関する随想
2025 年 7 月号	• 未成年者の心身の健康に影響を与える可能性のあるインターネット情報分類方法（意見募集稿） • 反不正競争法	• 訪日外客の構成に思うこと
2025 年 6 月号	• 医療広告監督管理ガイドライン • ライブコマース監督管理弁法（意見募集稿）	• EU が中国の禁訴令を WTO 提訴している事案の進展 • 中国個人情報保護コンプライアンス監査弁法と関連法令の整理 • ラブブの背景にある中国のグッズ経済
2025 年 5 月号	• 中華人民共和国民営経済促進法 • 営業秘密保護規定（意見募集稿）	• 上海における電気自動車の普及
2025 年 4 月号	• 顔識別技術応用安全管理弁法 • 企業経営異常名簿管理弁法及び企業公示情報抜取検査弁法の改正	• 中国における生成 AI 規制 • 中国が米インフレ削減法を WTO 提訴している事案の進展 • 流砂の歩き方を学ぶ
2025 年 3 月号	• 個人情報保護コンプライアンス監査管理弁法 • 『中華人民共和国会社法』に基づく会社登録強制抹消登記制度の実施に関する規定（意見募集稿）	• 日本と中国のコンテンツ業界における新たな潮流
2025 年 2 月号	• 外貨及び香港、マカオ、台湾通貨に係わる遅延支払の利息計算基準に関する最高人民法院の回答 • 医薬企業における商業賄賂リスクの防止に関するコンプライアンスガイ	• AI とうまく付き合う法

号数	紹介法令/判例	今月の中国関連ブログ記事／連載・コラム
	ドライン	
2025 年 1 月号	• 中華人民共和国増値税法 • 水平型事業者集中審査ガイドライン • 個人情報越境移転保護認証弁法（意見募集稿）	• 最近感じた傾向と中国ビジネスの展望
2024 年 12 月号	• 海外医薬品流通許可保有者による国内責任者の指定の管理に関する暫定規定 • モバイルインターネットにおける未成年者モード設定に関するガイドライン	• 日中間の入国手続の緩和
2024 年 11 月号	• 外国投資者の中国上場企業への戦略投資に関する管理弁法 • 商標権侵害案件違法経営額計算弁法 • 「全国祝祭日及び記念日休暇弁法」改正に関する決定	• 【商標】不使用取消請求の審査に関する新動向 • 両用品目輸出管理条例及び両用品目輸出管理リスト • 中国「双十一」セールにおける３つの変化
2024 年 10 月号	• ネットワークデータ安全管理条例 • 最高人民法院による＜中華人民共和国民法典＞の不法行為編の適用に関する解釈（一）	• センシティブ個人情報識別ガイドラインとネットワークデータ安全管理条例の公表 • 標準契約条項の届出実務を振り返って

編集・発行
TMI 総合法律事務所
発行日
2025 年 10 月 31 日

TMI 総合法律事務所中国プラクティスグループ

東京オフィス
〒106-6123 東京都港区六本木 6-10-1
六本木ヒルズ森タワー23 階
TEL: +81-(0)3-6438-5511
E-mail: chinalaw@tmi.gr.jp

上海オフィス
〒200031 上海市徐匯区淮海中路 1045 号
淮海国際広場 2605 室
TEL: +86-(0)21-5465-2233
E-mail: shanghai@tmi.gr.jp

北京オフィス
〒100020 北京市朝陽区東三環中路 9 号
富爾大厦 3204 室
TEL：+86-(0)10-8595-1435
E-mail: beijing@tmi.gr.jp

TMI 総合法律事務所拠点一覧

オフィス
東京/名古屋/大阪/京都/神戸/広島/福岡/上海/北京/ヤンゴン/シンガポール/ホーチミン/ハノイ/プノンペン/バンコク/シリコンバレー/ロンドン/パリ/ブリュッセル/ジャカルタ/クアラルンプール/シドニー※
現地デスク
フィリピン/ブラジル/メキシコ/ケニア

※ジャカルタ及びクアラルンプールは現地法律事務所との提携による