個人情報保護コンプライアンス監査管理弁法（パブリックコメント案）の公表

２０２３年８月７日
桃尾・松尾・難波法律事務所
パートナー弁護士・北京大学法学博士　松尾剛行[1]
（Email:mmn@mmn-law.gr.jp）
フォーリン・リーガル・スタッフ　楊燦燦[2]
（Email: Yang.Cancan@mmn-law.gr.jp）

弊事務所では中国個人情報保護法について様々なニュースレターを公開してきた[3]。２０２３年３月には、いわゆるSCC(中国個人情報越境標準契約)についてニュースレターを公開したところである[4]。そして、中国個人情報保護法についてまた新しい重要な動きがあった。すなわち、同年８月３日、インターネット情報弁公室は、個人情報保護コンプライアンス監査管理弁法（パブリックコメント案）（个人信息保护合规审计管理办法（征求意见稿）。以下、「本弁法」という。）を公表した。日本企業の中国子会社のような一般的な個人情報処理者も、２年に１度の監査を行わなければならない等、実務への影響が大きいことから、以下簡単に紹介したい。

１　背景

２０２１年１１月の中国個人情報保護法[5]施行後、個人情報保護法を処理する者（個人情報処理者、ほぼ全ての中国企業と域外適用を受ける外国企業を含む）は、個人情報保護法を遵守する必要がある。しかし、実際には個人情報保護法に違反する企業は後を絶たず、処罰事例も既に存在する[6]。

このような状況において、もちろん個別の事案の処罰を行うことも一つの重要な対応策であるが、これに加え、各社が内部においてコンプライアンス活動を実施し、各社においてきちんと個人情報保護法を遵守しているかを監査することで、規制当局としては、より少ない資源で個人情報保護の実効性を高めることができる。

そこで、本弁法は、個人情報処理者の個人情報処理活動が法律及び行政法規に適合しているかどうかを調査・評価する監督活動を個人情報保護コンプライアンス監査（本弁法３条）と定義

---

[1] 第一東京弁護士会。NY州弁護士。
[2] 中国司法試験合格者。
[3] https://www.mmn-law.gr.jp/about/global/china/index.html　に列挙している。
[4] https://www.mmn-law.gr.jp/assets/pdf/20230307_client.pdf
[5] 石本・松尾他『中国デジタル戦略と法』参照。また、https://www.mmn-law.gr.jp/assets/pdf/20210906_client.pdf も参照。
[6] 例えば、2023年7月19日付けの経公（華）行罰決決字〔2023〕698号行政処罰決定書によれば、無錫におけるある企業が個人情報を保護する義務を尽くさず、内部管理制度等を定めていなかったため、当局は同社に対し警告をし、５日以内に改善するよう命じ、暫定的にアプリのサービスを停止するよう命じた。

した上で、その監督管理に関するルールを定めた（本弁法２条参照)。

２　監査実施義務

実務上影響が大きいのは監査実施義務（本弁法４条）である。すなわち本弁法４条は、「１００万人以上の個人情報を取り扱う個人情報処理事業者は、少なくとも１年に１回、その他の個人情報処理事業者は、少なくとも２年に１回、個人情報保護コンプライアンス監査を実施しなければならない。」と規定し、１００万人以上の個人情報を取り扱うならば年１回以上、それ以外の場合であっても２年に１回以上の監査実施義務を定めている。このような定期的監査に加え、比較的大きなリスクの存在やセキュリティインシデントの発生を理由に当局からの指示があれば､専門機構に委託して個人情報保護コンプライアンス監査を実施しなければならない(本弁法６条)。専門機関は独立性と客観性を保持するため、同一の個人情報処理者に連続して３回を超えて個人情報保護コンプライアンス監査を実施してはならない（本弁法１２条)。

３　監査方法

定期監査であれば、監査方法は自主監査でも専門機関に委託しての監査でもどちらでも良い（本弁法５条)。

しかし、当局からの指示による場合は専門機関に委託しなければならず（本弁法６条)、個人情報処理者は専門機関が適切に権限を行使できるようにしなければならず（本弁法８条)、終了後個人情報保護コンプライアンス監査報告書を当局に提出しなければならない(本弁法１０条)。かつ、専門機関が提示した是正案に従って是正を行い、専門機関の審査を経て、当局に是正状況を報告しなければならない（本弁法１１条)。

４　監査上の参考となるポイント

本弁法別紙ではかなり詳細に、監査上の参考となるポイントについて列挙している。本ニュースレターではその詳細は個別に紹介しないものの、例えば、プライバシーポリシーのように処理ルールを制定する方法で個人情報処理の基本原則を告知する場合（個人情報保護法１７条３項）については、別紙３条が以下のとおりポイントを列挙している。

・個人情報処理者の氏名又は名称及び連絡先が、真実、正確かつ完全に伝達されているかどうか
・収集する個人情報並びにその処理の目的、方法及び範囲が一覧表の形式によって明確に定められているかどうか
・個人情報の保存期間又は保存期間の決定方法、保存期間経過後の取扱方法を明確にしているかどうか、及び保存期間が取扱目的の達成に必要な最短の期間であることを確保しているか
・個人情報へのアクセス、コピー、加工、転送、訂正、補足、削除、開示、取扱いの制限、アカウントの取り消し、同意の撤回などのやり方及び方法が明確化されているかどうか；
・個人情報を第三者に提供する場合、提供先の氏名又は名称、連絡先、利用目的、利用方法及び個人情報の種類を明示しているか、個別に本人の同意を得ているか；
・その他法律及び行政法規に定める事項

今後は、本弁法別紙が個人情報保護に関するベストプラクティスを定めるものとして扱われることになる可能性が高いだろう。

５　実務対応

本弁法はパブリックコメント募集案に過ぎない。もっとも、日本企業としては自社の子会社について、今後最低でも２年に１度、場合によっては年１度や当局から指示があったタイミン

グにおいての個人情報保護コンプラインス監査が必要になることを踏まえて対応しなければならない。

そして、本弁法別紙は監査の際におけるいわばチェックリストとして働くだけではなく、いわば個人情報保護のための活動を遂行する上でのベストプラクティスとして扱われる可能性が高いことから、監査を行う場面だけではなく、例えばプライバシーポリシーを改訂する場合等においても、これらの項目を満たす形で改訂していくことが望ましいだろう。

とは言え、本弁法は現時点ではパブリックコメント案に過ぎない。今後正式版になるまでの間に、内容が変更される可能性もある。その意味では、今後もこれらの状況の変化に注目が必要である。

以上