個人情報保護コンプライアンス監査管理弁法

（国家インターネット情報弁公室令第 18 号として 2025 年 2 月 12 日発布、同年 5 月 1 日施行）

第 1 条　個人情報保護コンプライアンス監査活動を規範化し、個人情報に係る権益を保護するため、「中華人民共和国個人情報保護法」、「ネットワークデータ安全管理条例」等の法律・行政法規に基づき、本弁法を制定する。

第 2 条　中華人民共和国国内において、個人情報保護コンプライアンス監査を展開する際に、本弁法を適用する。

本弁法において「個人情報保護コンプライアンス監査」とは、個人情報処理者の個人情報処理活動が法律・行政法規を遵守しているか否かに係る状況に対して審査及び評価を行う監督活動をいう。

第 3 条　個人情報処理者は、個人情報保護コンプライアンス監査を自ら展開する場合には、個人情報処理者の内部機構が、又は専門機構に委託し、自身の個人情報処理に係る法律・行政法規遵守の状況に対してコンプライアンス監査を定期的に行わなければならない。

第 4 条　1000 万人分を超える個人情報を処理する個人情報処理者は、個人情報保護コンプライアンス監査を 2 年毎に少なくとも 1 回展開しなければならない。

第 5 条　個人情報処理者に次の各号に掲げる事由のいずれかがある場合には、国のネット情報部門及びその他の個人情報保護職責履行部門（以下「保護部門」と総称する。）は、個人情報処理活動に対するコンプライアンス監査の実施を専門機構に委託するよう個人情報処理者に要求することができる。

（一）　個人情報処理活動に、個人の権益に著しく影響し、又は安全措置を著しく欠く等の比較的大きいリスクが存在することを発見した場合

（二）　個人情報処理活動が、多数の個人の権益を侵害するおそれがある場合

（三）　個人情報セキュリティインシデントが発生し、100 万人分以上の個人情報又は 10 万人分以上の機微な個人情報が漏洩、改ざん、紛失又は毀損されることとなった場合

同一の個人情報セキュリティインシデント又はリスクに対して、個人情報保護コンプライアンス監査の展開を専門機構に委託するよう、個人情報処理者に重ねて要求してはならない。

第 6 条　個人情報処理者は、個人情報保護コンプライアンス監査を自ら展開し、又は保護部門の要求に従って専門機構に委託し展開させる場合には、本弁法の付属文書「個人情報保護コンプライアンス監査指針」を参照しなければならない。

第 7 条　専門機構は、個人情報保護コンプライアンス監査を展開する能力を備え、サービスと見合う監査人員、場所、施設及び資金等を有しなければならない。

関連専門機構が認証に合格していることを奨励する。専門機構の認証は、「中華人民共

和国認証認可条例」の関係規定に従って執行する。

第 8 条　個人情報処理者は、保護部門の要求に従って個人情報保護コンプライアンス監査を展開する場合には、専門機構が個人情報保護コンプライアンス監査業務を正常に展開するために必要なサポートを提供し、かつ、監査費用を負担しなければならない。

第 9 条　個人情報処理者は、保護部門の要求に従って個人情報保護コンプライアンス監査を展開する場合には、保護部門の要求に従って専門機構を選定し、限られた期間内に個人情報保護コンプライアンス監査を完了させなければならない。状況が複雑である場合には、保護部門に報告して承認を受けた後、適宜延長することができる。

第 10 条　個人情報処理者は、保護部門の要求に従って個人情報保護コンプライアンス監査を展開する場合には、コンプライアンス監査完了後に、専門機構が作成した個人情報保護コンプライアンス監査報告を保護部門に送付しなければならない。

個人情報保護コンプライアンス監査報告には、専門機構の主要責任者及びコンプライアンス監査責任者が署名し、かつ、専門機構公印を押捺しなければならない。

第 11 条　個人情報処理者は、保護部門の要求に従って個人情報保護コンプライアンス監査を展開する場合には、保護部門の要求に従って、コンプライアンス監査中に発見した問題に対し、是正を行わなければならない。是正完了後 15 業務日内に、保護部門に是正状況報告を送付する。

第 12 条　100 万人分以上の個人情報を処理する個人情報処理者は、個人情報保護責任者を指定し、個人情報処理者の個人情報保護コンプライアンス監査業務に責任を負わせなければならない。

重要なインターネットプラットフォームサービスを提供しており、ユーザー数が莫大で、かつ、業務類型が複雑な個人情報処理者は、主に外部の構成員により組織される独立機構を設立し、個人情報保護コンプライアンス監査の状況に対して監督を行わせなければならない。

第 13 条　専門機構は、個人情報保護コンプライアンス監査活動に従事する際においては、法律法規を遵守し、信義に従い誠実に取り組み、コンプライアンス監査に係る職業的専門家としての判断を公正かつ客観的に下さなければならず、個人情報保護コンプライアンス監査職責の履行中に得た個人情報、商業秘密、秘密保持商務情報等に対しては、法により秘密を保持しなければならず、漏洩又は他人への不法な提供をしてはならず、コンプライアンス監査業務終了後に関連情報を遅滞なく削除する。

第 14 条　専門機構は、個人情報保護コンプライアンス監査の展開を他の機構に再委託してはならない。

第 15 条　同一の専門機構及びその関連機構並びに同一のコンプライアンス監査責任者は、同一の監査対象に対し、個人情報保護コンプライアンス監査を連続して 3 回以上展開してはならない。

第 16 条　保護部門は、個人情報処理者による個人情報保護コンプライアンス監査の展開状況に対して監督検査を行う。

第 17 条　いかなる組織及び個人も、個人情報保護コンプライアンス監査中の違法活動について、保護部門に苦情申立・通報を行う権利を有する。苦情申立・通報を受けた部門は、法により遅滞なく処理し、かつ、処理結果を苦情申立・通報者に告知しなければならない。

第 18 条　個人情報処理者又は専門機構が本弁法の規定に違反する場合には、「中華人民共和国個人情報保護法」、「ネットワークデータ安全管理条例」等の法律法規の規定により処理する。犯罪を構成する場合には、法により刑事責任を追及する。

第 19 条　国家機関及び法律・法規により授権された、公共事務を管理する職能を有する組織に対する個人情報保護コンプライアンス監査については、本弁法を適用しない。

第 20 条　本弁法は、2025 年 5 月 1 日から施行する。

付属文書

個人情報保護コンプライアンス監査指針

一、本指針は、「中華人民共和国個人情報保護法」、「ネットワークデータ安全管理条例」等の法律・行政法規に基づいて制定する。

二、個人情報処理活動の適法性の根拠に対してコンプライアンス監査を行う場合には、次の各号に掲げる事項を重点的に審査しなければならない。

（一） 個人の同意に基づき個人情報を処理する場合に、個人の同意を取得しているか否か。当該同意は個人が十分に情報を与えられているという前提の下で、自由意思により、かつ明確になされたか否か

（二） 個人の同意に基づき個人情報を処理する場合において、個人情報の処理目的、処理方式及び処理する個人情報の種類に変更が生じたときに、個人の同意を新たに取得しているか否か

（三） 個人の同意に基づき個人情報を処理する場合に、法律・行政法規により、個人の単独の同意又は書面による同意を取得しているか否か

（四） 個人情報を処理するのに個人の同意を取得していないものは、法律・行政法規の規定により、個人の同意を取得する必要がない事由に該当するか否か

三、個人情報処理規則に対してコンプライアンス監査を行う場合には、次の各号に掲げる事項を重点的に審査しなければならない。

（一） 個人情報処理者の名称又は氏名及び連絡先を真実、正確かつ完全に告知しているか否か

（二） リスト等の見やすい形式をもって、収集した個人情報並びにその処理方式及び種類を明記しているか否か

（三） 処理目的と直接関連しており、個人の権益に対する影響が最小である方式を採用しているか否か

（四） 個人情報の保存期間又は保存期間の確定方法及び期限到来後の処理方式を明確にし、並びに保存期間は処理目的を実現するのに必要な最短の期間で確定しているか否か

（五） 個人が個人情報を閲覧、複製、移転、訂正、補足、削除及び処理制限する場合並びにアカウント抹消及び同意撤回をする場合のルート及び方法が明確であるか否か

四、個人情報処理者による個人情報処理規則の告知義務の履行に対してコンプライアンス監査を行う場合には、次の各号に掲げる事項を重点的に審査しなければならない。

（一） 個人情報処理者が個人情報を処理する前に、目立つ方式及び明瞭で分かりやすい言葉により、真実、正確かつ完全に、個人情報処理規則を個人に告知しているか否か

（二） 告知文のサイズ、フォント及び色は、個人が告知事項を完全に閲読するのに便宜が図られているか否か

（三） オフライン告知では、注釈、説明等の複数の方式を通じて個人に対し告知義務を履行しているか否か

（四） オンライン告知では、テキスト情報を提供し、又は適当な方式を通じて、個人に

対し告知義務を履行しているか否か

（五） 個人情報処理規則に変更が生じた場合に、変更内容を個人に遅滞なく告知しているか否か

（六） 個人情報を処理するのに告知が不要とされているものは、法律・行政法規の規定により、秘密を保持しなければならない、又は告知する必要がない事由に該当するか否か

五、個人情報処理者による他の個人情報処理者との個人情報の共同処理に対してコンプライアンス監査を行う場合には、次の各号に掲げる事項を重点的に審査しなければならない。

（一） 各自の権利義務を約定しているか否か

（二） 個人情報の権益保護メカニズム

（三） 個人情報セキュリティインシデントの報告メカニズム

（四） その他法律・行政法規の規定により約定する必要がある権利及び義務

六、個人情報処理者による個人情報の処理の委託に対してコンプライアンス監査を行う場合には、次の各号に掲げる事項を重点的に審査しなければならない。

（一） 個人情報処理者は、個人情報の処理を委託する前に、個人情報保護影響評価を展開しているか否か

（二） 個人情報処理者が受託者と締結した契約は、処理を委託する目的、期間、方式、個人情報の種類、保護措置及び双方の権利義務等を受託者と約定しているか否か

（三） 個人情報処理者は、定期検査等の方式を採用して、受託者の個人情報処理活動に対し監督を行っているか否か

七、個人情報処理者に、合併、再編、分割、解散、破産被宣告等の原因により個人情報を移転する必要がある事由が存在する場合には、個人情報処理者が受領者の名称又は氏名及び連絡先を個人に告知しているか否かを重点的に審査しなければならない。

八、その処理する個人情報の個人情報処理者から他の個人情報処理者への提供に対してコンプライアンス監査を行う場合には、次の各号に掲げる事項を重点的に審査しなければならない。

（一） 個人の同意に基づいて個人情報を処理する場合に、個人の単独の同意を取得しているか否か

（二） 受領者の名称又は氏名、連絡先、処理目的、処理方式及び個人情報の種類を個人に告知しているか否か（法律・行政法規の規定により秘密を保持しなければならず、又は告知する必要がない場合を除く。）

（三） 個人情報保護影響評価を事前に行っているか否か

九、個人情報処理者による自動化された意思決定を利用した個人情報の処理に対してコンプライアンス監査を行う場合には、次の各号に掲げる事項を重点的に審査しなければならない。

（一） 自動化された意思決定の透明性及び自動化された意思決定の結果が公平・公正であるか否か

（二） 自動化された意思決定により処理する個人情報の種類及びもたらされる可能性のある影響を事前に個人に告知しているか否か

（三） 個人情報保護影響評価を事前に行っているか否か

（四） 個人の権益に重大な影響がある決定を自動化された意思決定の方式を通じて行うことを個人が簡便な方式により拒絶することができ、かつ、ユーザー個人の権益に重大な影響がある決定を自動化された意思決定の方式を通じて行うことについての説明を個人情報処理者に要求することができるよう、ユーザーに保障メカニズムを提供しているか否か

（五） 個人に情報配信又は商業的マーケティングを行う場合に、個人的な特徴に焦点を定めていない選択肢を同時に提供し、又は自動化された意思決定サービスを拒絶する簡便な方式を提供しているか否か

（六） 自動化された意思決定により、消費者の嗜好、取引習慣等に基づき、取引条件上、個人に対して不合理な差をつけた待遇が実行されることを、有効な措置を講じて防止しているか否か

（七） その他自動化された意思決定の透明性並びに結果の公平性及び公正性に影響を与える可能性のある事項

十、個人情報処理者による個人の同意に基づいた個人情報の公開に対してコンプライアンス監査を行う場合には、次の各号に掲げる事項を重点的に審査しなければならない。

（一） 個人情報処理者がその処理する個人情報を公開する前に、個人の単独の同意を取得しているか否か。当該授権は、真実かつ有効であるか否か。個人の意思に反して個人情報を公開している状況があるか否か

（二） 個人情報処理者が個人情報を公開する前に、個人情報保護影響評価を行っているか否か

十一、個人情報処理者が公共の場所において画像収集及び個人の身分識別設備を据え付ける場合には、その画像収集及び個人情報身分識別設備の据付けに係る適法性並びに収集した個人情報の用途に対して重点的に審査を行わなければならない。審査内容には、次の各号に掲げるものをそれらに限定することなく含む。

（一） 公共の安全を維持するのに必要か否か。収集した個人情報を商業目的のために処理するか否か

（二） 目立つ注意喚起標識を設置しているか否か

（三） 個人情報処理者が収集した個人の画像又は身分識別情報が公共の安全の維持以外の用途に用いられる場合には、個人の単独の同意を取得しているか否か

十二、個人情報処理者による既に公開されている個人情報の処理に対してコンプライアンス監査を行う場合には、次の各号に掲げる違法・規定違反行為が個人情報処理者にあるか否かを重点的に審査しなければならない。

（一）既に公開されている個人情報中の電子メールアドレス、携帯電話番号等に対して、その公開目的と関係のない商業情報を送信すること。

（二） 既に公開されている個人情報を利用し、サイバー暴力、ネット上のデマ及び虚偽情報を流す等の活動に従事すること。

（三） 既に公開されている個人情報で、処理することを個人が明確に拒絶しているものを処理すること。

（四）個人の権益に重大な影響がある場合において、個人の同意を取得していないこと。

（五） 既に公開されている個人情報を収集、保管又は処理する規模、期間又は使用目的が合理的な範囲を逸脱していること。

十三、個人情報処理者による機微な個人情報の処理に対してコンプライアンス監査を行う場合には、次の各号に掲げる事項を重点的に審査しなければならない。

（一） 個人の同意に基づき個人情報を処理する場合において、生体識別、宗教信仰、特定の身分、医療健康、金融口座、移動軌跡等の機微な個人情報を処理するときに、個人の単独の同意を事前に取得しているか否か

（二） 個人の同意に基づき個人情報を処理する場合において、14 歳に満たない未成年者の個人情報を処理するときに、未成年者の父母その他の保護者の同意を事前に取得しているか否か

（三） 機微な個人情報を処理する目的、方式及び範囲が適法・正当・必要であるか否か

（四） 個人情報保護影響評価を事前に行っているか否か

（五） 機微な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を、個人に告知しているか否か（法律・行政法規の規定により秘密を保持しなければならず、又は告知する必要がない場合を除く。）

（六） 法律・行政法規の規定により書面による同意を取得しなければならない場合に、書面による同意を取得しているか否か

（七） 機微な個人情報の処理に対する法律・行政法規の制限規定を遵守しているか否か

十四、個人情報処理者による 14 歳に満たない未成年者の個人情報の処理に対してコンプライアンス監査を行う場合には、次の各号に掲げる事項を重点的に審査しなければならない。

（一） 専門の個人情報処理規則を制定しているか否か

（二） 未成年者の個人情報の処理目的、処理方式、処理の必要性、及び処理する個人情報の種類、講じる保護措施等を未成年者及びその保護者に告知しているか否か（法律・行政法規の規定により告知する必要がない場合を除く。）

（三） 個人の同意に基づいて個人情報を処理する場合に、不必要な個人情報の処理への同意を未成年者又はその保護者に強要する行為があるか否か

十五、個人情報処理者による個人情報の国外への提供に対してコンプライアンス監査を行う場合には、次の各号に掲げる事項を重点的に審査しなければならない。

（一） 重要な情報インフラの運営者による個人情報の国外への提供について、国のネット情報部門が組織する安全評価を経ているか否か（法律・行政法規又は国のネット情報部門に別段の規定がある場合には、当該規定に従う。）

（二） 重要な情報インフラの運営者以外のデータ処理者による当該年度の 1 月 1 日から累計で 100 万人分以上の個人情報（機微な個人情報を含まない。）又は 1 万人分以上の機微な個人情報の国外への提供について、国のネット情報部門が組織する安全評価を経ているか否か（法律・行政法規又は国のネット情報部門に別段の規定がある場合には、当該規定に従う。）

（三） 重要な情報インフラの運営者以外のデータ処理者が当該年度の 1 月 1 日から累計で 10 万人分以上かつ 100 万人分に満たない個人情報（機微な個人情報を含まない。）又は 1 万人分に満たない機微な個人情報を国外へ提供する場合に、国のネット情報部門の規定に従い個人情報保護認証を経ているか、若しくは国のネット情報部門が制定する標準契約に従い国外受領者と契約を締結し、かつ、所在地の省級ネット情報部門に届け出ているか、又は法律・行政法規若しくは国のネッ

ト情報部門が定めるその他の条件に適合しているか否か

（四） 中華人民共和国国内に保存されている個人情報を外国の司法又は法執行機構に提供する事由がある場合に、中華人民共和国主管機関の承認を経ているか否か

（五） 個人情報提供の制限又は禁止に係るリストに組み入れられている組織及び個人に個人情報を提供しているか否か

十六、個人情報削除権の保障状況に対してコンプライアンス監査を行う場合には、次の各号に掲げる事項を重点的に審査しなければならない。

（一） 個人情報処理目的が既に実現され、若しくは実現不可能となり、又は処理目的の実現のために必要でなくなったか否か

（二） 個人情報処理者が製品若しくはサービスの提供を停止しているか否か、又は個人がアカウントを既に抹消しているか否か

（三） 保存期間が既に満了しているか否か

（四） 個人が同意を撤回しているか否か

（五） 個人情報処理者が法律・行政法規に違反し、又は約定に違反して個人情報を処理しているか否か

（六） 個人情報を削除しなければならないが、法律・行政法規で定める保存期間が満了せず、又は個人情報の削除が技術的に実現困難な場合に、保存及び必要な安全措置の採用以外の処理を個人情報処理者が停止したか否か

十七、個人情報処理活動中における個人の権利についての個人情報処理者による保障状況に対してコンプライアンス監査を行う場合には、次の各号に掲げる事項を重点的に審査しなければならない。

（一） 個人の権利行使に係る簡便な申請受理メカニズム及び処理メカニズムを確立しているか否か

（二） 個人の権利行使に係る申請に遅滞なく対応しているか否か。処理意見又は執行結果を遅滞なく完全かつ正確に告知しているか否か

（三） 個人の権利行使に係る請求を拒絶する場合に、個人に理由を説明しているか否か

十八、個人情報処理者は、個人の申請に対応し、その個人情報処理規則に対して説明を行わなければならず、コンプライアンス監査の際には次の各号に掲げる内容について重点的に評価を行わなければならない。

（一） 個人情報処理者が簡便な方式及びルートを提供し、個人情報処理規則の説明に関する個人の要求を受け付け、及び処理しているか否か

（二） 個人の要求を受けた後、個人情報処理者が合理的な期間内に、平易な言葉を使用して、その個人情報処理規則に対し説明をしているか否か

十九、個人情報処理者は、法律・行政法規の規定により内部管理制度及び操作規程を制定し、組織構造及び職位職責を明確にし、業務フローを確立し、及び内部統制制度を完全化して、個人情報処理に係るコンプライアンス及びセキュリティを保障しなければならない。コンプライアンス監査の際には、次の各号に掲げるものを含むがそれらに限らず、個人情報処理者の個人情報保護に係る内部管理制度及び操作規程に対して重点的に審査を行わなければならない。

（一） 個人情報保護業務の方針、目標及び原則が法律・行政法規の規定に適合しているか否か

（二） 個人情報保護に係る組織構造、人員配置、行為規範及び管理責任が、履行すべき個人情報保護責任と見合うものか否か
（三） 個人情報の種類、出所、機微度、用途等に基づき、個人情報に対して分類を行っているか否か
（四） 個人情報セキュリティインシデント緊急時対応メカニズムを確立しているか否か
（五） 個人情報保護影響評価制度及びコンプライアンス監査制度を確立しているか否か
（六） 個人情報保護に係る円滑な苦情申立通報受理フローを確立しているか否か
（七） 個人情報処理に係る操作権限を合理的に制定しているか否か
（八） 個人情報保護に係る安全教育及び研修計画を制定して実施しているか否か
（九） 個人情報保護責任者及び関連人員の職務履行評価制度を確立しているか否か
（十） 個人情報違法処理責任制度を確立しているか否か
（十一）法律・行政法規で定めるその他の事項

二十、個人情報処理者は、処理する個人情報の規模・類型と見合う安全技術措置を講じなければならず、かつ、個人情報処理者が講じる技術措置の有効性に対して評価を行う場合には、評価内容に、次の各号に掲げるものをそれらに限定することなく含む。
（一） 相応の安全技術措置を講じて個人情報の機密性、完全性及び可用性を実現しているか否か
（二） 暗号化、非識別化等の安全技術措置を講じ、追加的な情報に依拠しない状況において、個人情報の識別可能性を除去又は低下させるよう確保しているか否か
（三） 講じた安全技術措置が、関係人員による個人情報の閲覧、複製、送信等の操作権限を合理的に確定し、個人情報の処理過程における授権を経ていないアクセス及び濫用のリスクを減少させることができるものであるか否か

二十一、個人情報処理者の教育研修計画の制定及び実施状況に対してコンプライアンス監査を行う際には、次の各号に掲げる事項に対して重点的に評価を行わなければならない。
（一） 計画に従い管理人員、技術人員、操作人員及び全人員に対して相応の安全教育及び研修を展開しているか否か。相応の人員の個人情報保護に係る意識及び技能に対して考査を行っているか否か
（二） 研修の内容、方式、対象、頻度等が、個人情報保護に係るニーズを充足することができるものであるか否か

二十二、個人情報処理者が指定した個人情報保護責任者の職務履行状況に対してコンプライアンス監査を行う場合には、次の各号に掲げる事項を重点的に審査しなければならない。
（一） 個人情報保護責任者が関連する業務経歴及び専門知識を有し、個人情報保護に関連する法律・行政法規を熟知しているか否か
（二） 個人情報保護責任者が明確ではっきりとした職責を有するか否か、個人情報処理者内部の関連部門及び人員を調整する十分な権限を与えられているか否か
（三） 個人情報保護責任者が個人情報処理に係る重大事項の意思決定前に、関連する意見及び提案を申し入れる権利を有するか否か
（四） 個人情報保護責任者が個人情報処理者内部の個人情報処理に係るコンプライア

ンスに反する操作に対して制止を行い、及び必要な是正措置を講じる権利を有するか否か

（五） 個人情報処理者が個人情報保護責任者の連絡先を公開し、かつ、個人情報保護責任者の氏名、連絡先等を保護部門に提出しているか否か

二十三、個人情報処理者による個人情報保護影響評価の展開状況に対してコンプライアンス監査を行う際には、影響評価の展開状況及び評価内容に対して重点的に審査を行わなければならない。

（一） 法律・行政法規の規定により、個人の権益に重大な影響を有する個人情報処理活動を行う前に、個人情報保護影響評価を行っているか否か

（二） 個人情報の処理目的、処理方式等に対して適法・正当・必要な評価を行っているか否か

（三） 個人の権益の影響及び安全リスクに対して評価を行っているか否か

（四） 講じた保護措置の適法性、有効性及びリスクの程度との相応性に対して評価を行っているか否か

二十四、個人情報処理者は、個人情報セキュリティインシデント緊急時対応案を制定しなければならない。コンプライアンス監査の際には、次の各号に掲げる内容を含むがそれらに限らず、緊急時対応案の全面性、有効性及び執行可能性に対して評価をしなければならない。

（一） 業務の実態を踏まえ、直面する個人情報安全リスクに対して体系的に評価及び予測をしているか否か

（二） 総体的要求・基本的方針、組織機構・人員、技術・物資の保障、指揮・処置の手順、緊急時対応及びサポート措置等が、予測されるリスクに対処するのに十分であるか否か

（三） 関連人員に対して緊急時対応案に係る研修を行い、緊急時対応案について定期的に訓練を行っているか否か

二十五、個人情報処理者による個人情報セキュリティインシデントに係る緊急対応処置の状況に対してコンプライアンス監査を行う場合には、次の各号に掲げる事項を重点的に審査しなければならない。

（一） 緊急時対応案及び操作規程に従って個人情報セキュリティインシデントの影響、範囲及びもたらされる可能性のある危害を遅滞なく明らかにし、インシデント発生の原因を分析及び確定し、危害拡大を防止する措置計画を打ち出しているか否か

（二） 通報ルートを確立し、セキュリティインシデント発生後に関連規定に従って保護部門及び個人に遅滞なく通知しているか否か

（三） 個人情報セキュリティインシデントがもたらす可能性のある損失及び生じる可能性のある危害のリスクを、相応の措置を講じて最小まで抑えているか否か

二十六、重要なインターネットプラットフォームサービスを提供し、ユーザー数が莫大で、かつ、業務類型が複雑な個人情報処理者が制定するプラットフォーム規則に対してコンプライアンス監査を行う場合には、次の各号に掲げる事項を重点的に審査しなければならない。

（一） プラットフォーム規則が法律・行政法規に抵触するか否か

（二） プラットフォーム規則の個人情報保護条項の有効性。プラットフォーム及びプラットフォーム内の製品又はサービス提供者の個人情報保護に係る権利及び義務を合理的に区分しているか否か

（三） プラットフォーム規則の執行状況。サンプリング等の方式を通じて、プラットフォーム規則が有効に執行されていることを検証しているか否か

二十七、重要なインターネットプラットフォームサービスを提供し、ユーザー数が莫大で、かつ、業務類型が複雑な個人情報処理者が発布する個人情報保護に係る社会的責任報告に対してコンプライアンス監査を行う場合には、次の各号に掲げる内容の社会的責任報告での開示状況を重点的に審査しなければならない。

（一） 個人情報保護に係る組織構造及び内部管理状況

（二） 個人情報保護能力の構築状況

（三） 個人情報保護措置及び成果

（四） 個人の権利行使に係る申請の受理状況

（五） 独立監督機構の職務履行状況

（六） 重大な個人情報セキュリティインシデントの処理状況

（七） 個人情報保護の社会共治に係る科学普及宣伝及び公益活動の促進状況

（八） 法律・行政法規で定めるその他の事項

（法令原文名称：个人信息保护合规审计管理办法）