日本DPO協会　第14回個人情報保護セミナー

# 中国のデータ越境移転規制について

2023年7月27日

牛島総合法律事務所
**弁護士　影島広泰**
hiroyasu.kageshima@ushijima-law.gr.jp
03-5511-3233

# お問い合わせ先


## 牛島総合法律事務所　弁護士　影島広泰

03-5511-3233
hiroyasu.kageshima@ushijima-law.gr.jp

東京都千代田区永田町2-11-1
　山王パークタワー14階


| | |
|---|---|
| 2003.10 | 弁護士登録（第56期）牛島総合法律事務所入所 |
| 2013.1 | 牛島総合法律事務所パートナー |
| 2015.5 | 情報化推進国民会議 本委員（～2017.3） |
| 2015.7 | 情報化推進国民会議 マイナンバー検討特別委員会委員（～2015.12） |
| 2017.4 | JIPDECプライバシーマーク付与適格性審査会委員 |

**【個人情報の取扱い・情報管理に関する案件】**
- **パーソナルデータを利用したビジネス構築のための法的スキームの助言**
- **内外企業がクロスボーダーにデータを移転する際の法的助言（GDPR・CCPA・アジア各国法）**

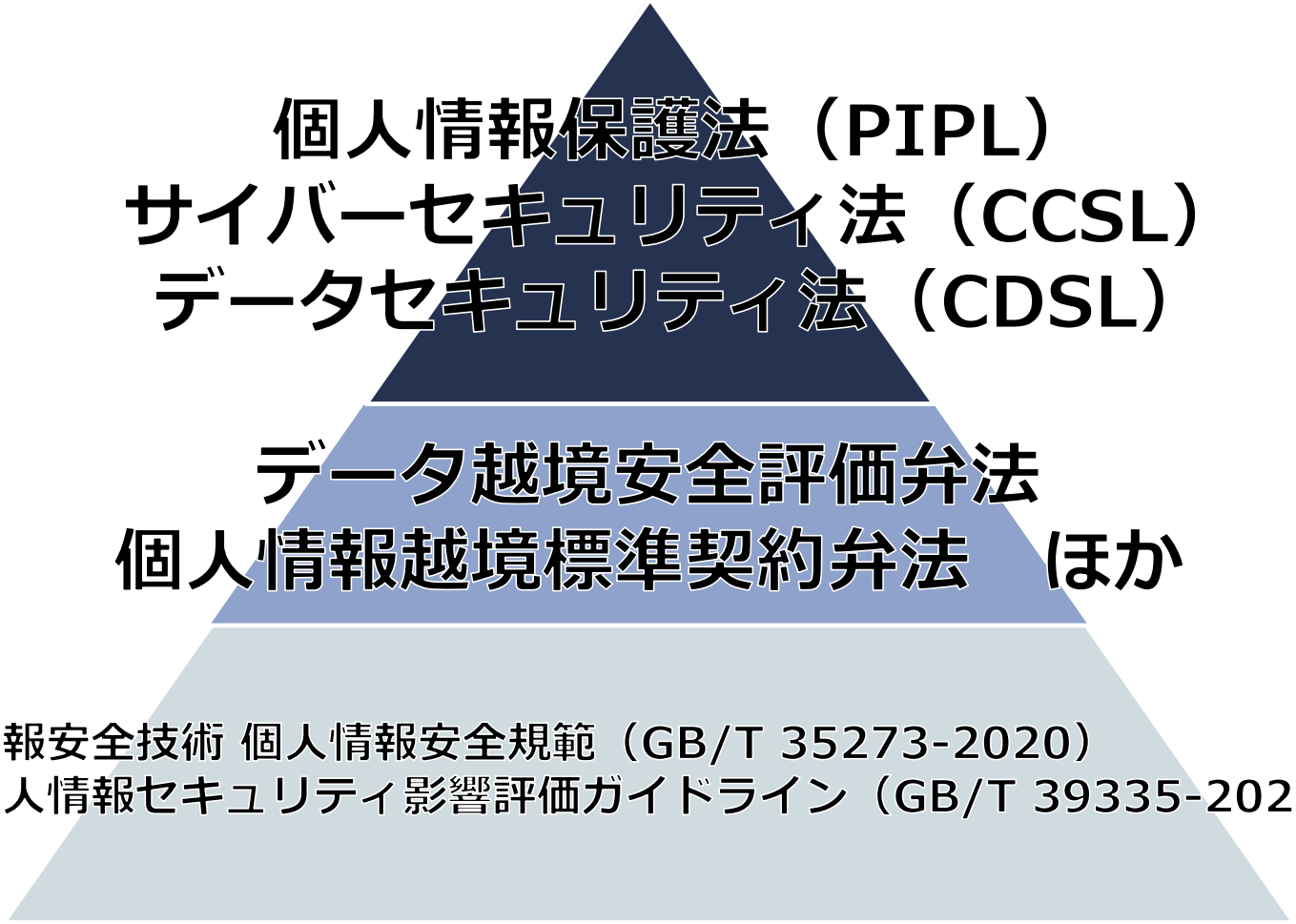
**【システム・ソフトウェア開発に関する案件】**
- **金融機関、流通、サービス業の各システム開発の中止に伴う訴訟・紛争**
- **システム開発プロジェクト遂行中のコスト増、品質問題、プロジェクト中断に関する交渉のアドバイス**

**【著作等】**
- **「法律家・法務担当者のためのIT技術用語辞典＜第2版＞」（商事法務）**
- **「座談会　システム開発取引はなぜ紛争が絶えないのか」（NBL1115～1117号）**
- **「個人情報保護法と企業実務」（清文社）ほか多数**

**【その他】**
- **Legal 500 Asia Pacific 2023年 TMT (Technology Media & Telecommunications)「Leading individuals」**
- **Thomson Reuters 2021年「ALB Asia Super 50 TMT Lawyers」に選出**
- **日本経済新聞社「企業法務・弁護士調査」2019年データ関連「企業が選ぶランキング」第1位**

# 目次

# 1. 中国のデータ3法



**法**

個人情報保護法（PIPL）
サイバーセキュリティ法（CCSL）
データセキュリティ法（CDSL）

**施行規則**

データ越境安全評価弁法
個人情報越境標準契約弁法　ほか

**規格（GB）**

・情報安全技術 個人情報安全規範（GB/T 35273-2020）
・個人情報セキュリティ影響評価ガイドライン（GB/T 39335-2020）ほか

# 2. 個人情報保護法
# (1) 総論

## ■ 個人情報の定義（4条）

「電子的その他の方法により記録された、特定された又は特定可能な自然人に関する各種情報であって、匿名化処理されたものを除く」

## ■ 域外適用あり（3条）

- 中華人民共和国国外において中華人民共和国国内の自然人の個人情報を処理する活動について、次の各号のいずれかに該当する場合にも、本法を適用する。
  - (1)国内の自然人に製品またはサービスを提供することを目的とする場合
  - (2)国内の自然人の行為を分析・評価する場合
  - (3)その他法律、行政法が定める場合

- 中国内に専門機関または指定代表を設立し、個人情報保護に関する事務の処理を担当し、個人情報保護責任を果たす部門に関係機関の名称または代表の氏名、連絡先などを届けなければならない（53条）

# 2. 個人情報保護法
# (1) 総論

➢ **個人情報の例（情報安全技術 個人情報安全規範（GB/T 35273-2020））**

| | |
|---|---|
| **基本的な個人情報** | 氏名、生年月日、性別、民族、国籍、家族関係、住所 電話番号、電子メールアドレスなど |
| **個人識別情報** | 身分証明書、軍人証明書、パスポート、運転免許証、社員証、パス、社会保障カード、住民票など |
| **個人バイオメトリクス情報** | 個人遺伝子、指紋、声紋、掌紋、耳介、虹彩、顔認識機能など |
| **オンライン識別情報** | 個人情報の対象者のアカウント、IPアドレス、個人用電子証明書 |
| **生理・健康情報** | 病理情報、入院記録、医師の指示、検査報告、手術・麻酔記録、看護記録、投薬記録、薬剤・食物アレルギー、不妊情報、病歴、診断・治療、家族病歴、現病歴、感染歴等の医療に関連する記録、体重・身長・肺活量等の個人健康情報 |
| **個人教育情報** | 個人の職業、地位、勤務先、学歴、学位、教育歴、職歴、研修歴、成績表など |
| **個人資産情報** | 銀行口座、認証情報（パスワード）、銀行預金情報（資金額、支払、回収記録等）、不動産情報、信用記録、取引・消費記録、銀行取引明細書等、および仮想通貨、仮想取引、ゲームCDキー等の仮想資産情報など |
| **個人コミュニケーション情報** | 通信記録およびコンテンツ、SMS、MMS、電子メール、個人的な通信を記述するデータ（しばしばメタデータと呼ばれる）など |
| **連絡先情報** | 連絡先、友達リスト、チャットグループのリスト、メールアドレスリストなど |
| **個人のウェブ閲覧記録** | ログに保存されたPI対象者の操作の記録（ウェブ閲覧記録、ソフトウェア使用記録、クリック記録、お気に入りなど）等を指す |
| **個人がよく使用する機器の情報** | ハードウェアのシリアル番号、機器のMACアドレス、ソフトウェアの一覧、機器固有の識別子（IMEI/Android ID/IDFA/Open UDID/GUID、SIMカードのIMSI情報）など、個人がよく使う機器の一般的な状態を記述した情報を指す |
| **個人の位置情報** | 居場所の記録、正確な位置情報、宿泊施設情報、経度・緯度などを含む |
| **その他の情報** | 結婚歴、宗教的嗜好、性的指向、未公表の犯罪歴など |

# 2. 個人情報保護法
# (2) 個人情報の取扱いに対する規制

## ■ 諸原則

- 個人情報の処理は合法、正当、必要及び誠実の原則を遵守しなければならず、ミスリード、詐欺、脅迫等の方式を通じて個人情報を処理してはならない（5条）
- 個人情報の処理は明確かつ合理的な目的を有し、かつ処理目的と直接関連し、個人権益に対する影響が最小の方式を採用しなければならない
  個人情報の収集は、取扱いの目的を達成するための最小限の範囲に限定し、過度に個人情報を収集してはならない （6条）
- 個人情報の処理は、公開、透明性の原則に従い、個人情報の処理規則を公開し、処理の目的、方式及び範囲を明示しなければならない（7条）
- 個人情報の処理は、個人情報の品質を保証し、個人情報の不正確・不完全による個人権益への不利な影響を回避しなければならない（8条）
- 個人情報取扱者は、その個人情報取扱行為について責任を負い、取り扱う個人情報の安全を確保するために必要な措置を講じなければならない（9条）
- いかなる組織、個人も他人の個人情報を不法に収集、使用、加工、伝送してはならず、他人の個人情報を不法に売買、提供又は公開してはならない、国家の安全、公共の利益に危害を及ぼす個人情報の処理活動に従事してはならない（10条）

# 2. 個人情報保護法
# (2) 個人情報の取扱いに対する規制

## ■ 処理の根拠（13条）

- 個人情報取扱者は、次のいずれかに該当する場合に限り、個人情報を取り扱うことができる。
  - （1）個人の同意を得た場合
  - （2）個人が一方の当事者としての契約を締結・履行するために必要であるか、または法律に基づく労働規章制度と法律に基づく集団契約 の下で人的資源管理を実施するために必要である場合
  - （3）法的役割または法的義務を果たすために必要である場合
  - （4）公衆衛生上の緊急事態に対応すること、または緊急時に自然人の生命、健康及び財産の安全を保護することが必要である場合
  - （5）公益の報道・世論監督などの行為を実施し、個人情報を適正な範囲で取り扱う場合
  - （6）本法の規定に従い、個人が自ら公開した、または他の、合法的に公開された個人情報を、合理的な範囲で処理する場合
  - （7）その他法律・行政法が定める場合
- 本法その他の関連規定によれば個人情報の取り扱いに個人の同意を取得すべきである場合であっても、前項2～7の適用がある場合は、個人の同意を取得する必要はない。

実務上、入社時に締結する労働契約に、個人情報の収集・利用とグループ企業内での共有についての条項を入れて同意を得ておくとよい。

# 2. 個人情報保護法
# (2) 個人情報の取扱いに対する規制

## ■ 情報提供（17条）

- 個人情報取扱者は、個人情報を取り扱う前に、次の事項を顕著な方法で、明確かつわかりやすい言語により、真実、正確かつ完全に個人に通知しなければならない。
  - （1）個人情報取扱者の氏名又は名称及び連絡先
  - （2）個人情報の処理目的、処理態様、処理する個人情報の種類、保存期限*
  - （3）個人がこの法律に基づいて権利を行使するための方法及び手順
  - （4）その他法律・行政法が告知すべきと定める事項

- 前項に規定する事項に変更が生じた場合、変更部分を個人に告知しなければならない。

- 個人情報取扱者は、個人情報処理規則を作成する方式で第一規定事項を通知する場合には、処理ルールを開示し、検索と保存が容易であるようにする。

＊「個人情報の保存期間は処理目的を達成するために必要な最短期間でなければならない」（19条）

# 2. 個人情報保護法
# (2) 個人情報の取扱いに対する規制

## ■ 委託先の監督（21条）

## ■ 第三者提供の同意（22条）

- 以下を告知し、個人の単独の同意を得なければならない。
  - ① 受取人の名称又は氏名
  - ② 連絡先
  - ③ 取扱目的
  - ④ 取扱方法
  - ⑤ 個人情報の種類
- 受取人は上述の処理目的、処理方式及び個人情報の種類等の範囲内で個人情報を処理しなければならない。
- 受取人が元の処理目的、処理方式を変更する場合、本法の規定に基づき改めて個人の同意を得なければならない。

## ■ 機微情報の取扱い（29条）

- 個人の個別の同意を得なければならない

## ■ 未成年者（31条）

- 14歳未満の未成年者個人情報を扱う場合は、未成年者の親または他の保護者から同意を得る必要がある

# 2. 個人情報保護法
# (2) 個人情報の取扱いに対する規制

## ■ 個人の権利

- 開示請求（45条）
- 不正確・不完全である場合の訂正・追加請求（46条）
- 削除義務・削除請求（47条）
  - ① 処理目的が実現され、実現できない、または実現するために必要ではない場合
  - ② 個人情報取扱者が製品やサービスの提供を停止したり、保存期間が満了する場合
  - ③ 個人が同意を撤回した場合
  - ④ 個人情報取扱者が法律、行政法規に違反したり、デフォルト規定に違反したりして個人情報を処理する場合
  - ⑤ 法律・行政法規定のその他の場合
- 取扱規程の説明を求める

# 2. 個人情報保護法
# (2) 個人情報の取扱いに対する規制

## ■ 情報管理等

- **安全管理措置（51条）**
  - ① 内部管理制度と操作規程を制定する
  - ② 個人情報を分類管理する
  - ③ 該当する暗号化、非識別化などの安全技術措置をとる
  - ④ 個人情報処理のアクセス権限を適切に定め、従業員に対して定期的に安全教育・訓練を行う
  - ⑤ 個人情報セキュリティ事象緊急事態対応予定案を作成し、組織化する
  - ⑥ その他法律・行政法が定める措置
- **規定数量に達した個人情報を処理する個人情報取扱者（52条）**
  **→個人情報保護責任者を指定し、監督責任を負わなければならない**
  - 個人情報保護責任者の連絡先を公開し、個人情報保護責任者の氏名、連絡先等を個人情報保護職責を履行する部門に送信・報告する義務
- **コンプライアンス監査の義務（54条）**
- **漏えい時の当局への報告及び本人への通知義務（57条）**

# 2. 個人情報保護法
# (2) 個人情報の取扱いに対する規制

## ■ 個人情報保護効果評価（PIA）（55条）

- **以下の場合に義務**
  - ① 機微個人情報を処理する場合
  - ② 個人情報を用いた自動的決定を行う場合
  - ③ 処理を委託し、他の個人情報取扱者に個人情報を提供し、又は個人情報を開示する場合
  - **④ 国外に個人情報を提供する場合**
  - ⑤ 個人権益に大きな影響を与える他の個人情報処理活動を行う場合
- **以下を評価**
  - ① 個人情報の処理目的、処理方式などが合法であり、適切かつ必要であるか
  - ② 個人的な権利への影響や安全上のリスク
  - ③ 採用した保護措置が合法、有効であり、かつリスクの程度に適応しているか
- **個人情報保護影響評価報告書および取り扱い記録は、少なくとも3年間保存する必要あり**
- **GB/T 39335-2020（ただし、個人情報保護法施行前に策定）**

# 2. 個人情報保護法
# (3) 国外移転

## ■ 国外移転

- 個人情報取扱者は、業務等の必要により、中華人民共和国国外に個人情報を提供する必要がある場合には、次のいずれかの条件を備えていなければならない（38条）
  （1）本法第40条の規定に基づく国家網信任部門による安全評価
  （2）国のネットワーク信任部門の規定に従い、専門機関を介して個人情報保護認証を行う
  （3）国のネットワーク信任部門が制定した標準契約に従い、国外受信者と契約を結び、双方の権利と義務を定める
  （4）法律、行政法規又は国のネットワーク部門が規定するその他の条件

- 中華人民共和国が締結又は参加する国際条約、協定に中華人民共和国国外に個人情報を提供する条件等について規定がある場合、その規定に基づき実施することができる。

- 個人情報取扱者は、国外受信者による個人情報の取扱いがこの法律に定める個人情報保護基準に適合することを確保するために必要な措置を講じなければならない。

# 2. 個人情報保護法
# (3) 国外移転

- 国外に個人情報を提供する場合、以下の事項を告知し、かつ個人の単独の同意を得なければならない（39条）
  - ① 国外受取人の名称又は氏名
  - ② 連絡先
  - ③ 処理目的
  - ④ 処理方式
  - ⑤ 個人情報の種類
  - ⑥ 個人が国外受取人に本法に規定する権利を行使する方式と手順等

- 重要な情報インフラの運営者 及び
  個人情報の処理が国のネットワーク部門の規定数量に達した個人情報取扱者
  - 国内で収集及び発生した個人情報を国内に保存しなければならない
  - 真に国外に提供する必要がある場合、国家インターネット通信部門が組織した安全評価を通過しなければならない
    （法律、行政法規及び国家インターネット通信部門が安全評価を行わなくてもよいと規定している場合、その規定に従う）（40条）

# 2. 個人情報保護法
# (4) 制裁

## ■ 制裁

**通常の場合**

- 本法の規定に違反し個人情報を取扱い、又は個人情報の取扱にあたって本法の規定する個人情報保護義務を履行しない場合、個人情報保護職責履行部門が是正を命じ、警告を与え、違法所得を没収し、違法に個人情報を取り扱うアプリケーションに対しサービス提供の暫定的中止又は停止を命じる。
- 是正しない場合、100万元以下の過料
- 直接責任を負う主管人員及びその他の直接責任人員は1万元～10万元の過料

**情状が重い場合**

- 省レベル以上の個人情報保護職責履行部門が是正を命じ、違法所得を没収し、かつ5000万元以下又は前年度の売上高の100分の5以下の過料
- 関連する業務を暫定的に停止し、又は業務を止めて整理し、関係主管部門に通報して関係する業務許可を取消し又は営業許可を取消すことができる
- 直接責任を負う主管人員及びその他の直接責任人員は10万元～100万元以下の過料
- 加えて、一定期間内において関連企業の董事、監事、高級管理職及び個人情報保護責任者を担当することを禁止することを決定することができる。

# 2. 個人情報保護法
# （5）個人情報安全規範（GB/T 35273-2020）

## ■ 情報安全技術 個人情報安全規範（GB/T 35273-2020）

- **2020年10月1日実施**
- **GB/Tは「推薦的国家標準」だが、民間企業を監督しサイバーセキュリティ法を執行する当局（CAC）が期待するベストプラクティスが記載されていると報道されている**

**①個人情報の収集**

- データ最小化の原則
- 個人情報を収集・使用する目的、方法及び範囲等のルールを本人に明確に通知した上で、同意を得る
- 機微情報の取得には、明確かつ明白な同意
- プライバシーポリシーの公開

  （8項目が列挙されており、別紙に詳細な記載例あり。クッキーやピクセルタグについての記載まで詳細な例が挙げられている。国外移転についての記載もある。）
- 同意画面の作り方なども、具体例が記載されている

# 2. 個人情報保護法
# （5）個人情報安全規範（GB/T 35273-2020）

**②個人情報の保管**

- 保持期間を最小限にする
- 匿名化する、機微情報の送信は暗号化
- 責任ある部署と人員を特定、PIAの実施、教育、セキュリティ監査
- 漏えい時等の通知・報告

**③個人情報の利用**

- アクセス制御
- 表示制限
- 目的外利用など

**④アクセス権**

- 削除、訂正等の権利

**⑤委託**

- 同意の範囲内で委託する
- 受託行為の個人情報セキュリティ評価
- 受託者の報告義務、再委託の承認、終了時の消去義務
- 契約の締結

# 2. 個人情報保護法
# （5）個人情報安全規範（GB/T 35273-2020）

## ➢ 機微情報の定義

- 漏洩、違法な提供、または悪用された場合、個人および財産の安全性を危険にさらし、個人的な評判、肉体的および精神的健康被害または差別的取扱いにつながる恐れが高い個人情報
  一般に14歳以下の子供の個人情報等は機微情報

＜機微情報の例＞

| | |
|---|---|
| **個人資産情報** | 銀行口座、認証情報（パスワード）、銀行預金情報（資金額、支払、回収記録を含む）、不動産情報、信用記録、信用情報、取引・消費記録、銀行明細等、仮想通貨、仮想トランザクション、ゲームCDキー等の仮想資産情報 |
| **個人の健康情報** | 病理情報、入院記録、医師の指示、検査報告書、手術・麻酔記録、看護記録、投薬記録、薬剤・食物アレルギー、不妊情報、既往歴、診断・治療、家族の病歴、現病歴、感染歴など、医療に関連して作成された記録 |
| **個人生体情報** | 遺伝子、指紋、声紋、掌紋、耳介、虹彩、顔認識機能等 |
| **個人識別情報** | IDカード、軍人証明書、パスポート、運転免許証、従業員ID、社会保障カード、住民票等 |
| **その他の情報** | 性的指向、婚姻歴、宗教的嗜好性、非公開の犯罪記録、通信記録および内容、連絡先、友人リスト、チャットグループのリスト、居場所の記録、ウェブ閲覧履歴、正確な位置情報、宿泊情報など |

# 3. サイバーセキュリティ法
# (1) 総論

## ■ 規制を受ける対象（2017年6月1日施行）

- 「情報ネットワーク運営者」
  → 「重要情報インフラ運営者」の場合は、義務が加重される

## ■ 定義

| | |
|---|---|
| 情報ネットワーク運営者 | 情報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 |
| 重要情報インフラ運営者 | 公共通信・情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政務等の重要分野、「破壊を受け、機能を喪失し、またはデータの漏えいが発生した場合に、国の安全、人民の生活、公共利益に重大な危険をもたらす可能性がある」分野における重要情報インフラの運営者 |
| 情報ネットワーク | コンピューターやその他の情報端末、関連設備等で生成され、一定の規則およびプログラムに基づき、データの収集、保存、転送、交換、処理を行うシステム |
| 個人情報 | 電磁その他の方法によって記録され、単独でまたはその他の情報と結合して、自然人の個人身分を識別できるあらゆる情報をいい、たとえば自然人の氏名、生年月日、身分証明書番号、個人生物識別情報、住所、電話番号等が含まれる |

# 3. サイバーセキュリティ法
# (1) 総論

- **情報ネットワーク運営者**
  - ① **情報ネットワークの所有者**
    固定電話会社、携帯電話会社　等
  - ② **情報ネットワークの管理者**
    イントラネットを有する企業、社内向けウェブサイトを有する企業　等
  - ③ **ネットワークサービス提供者**
    ショッピングサイト、SNS、検索エンジン、メッセージサービスの提供企業

- **なお、ネットワーク関連製品・サービス・設備・安全専用品の提供者には、別途義務が課せられている（22条以下）**

# 3. サイバーセキュリティ法
# (2) 情報ネットワーク運営者の義務

## ■ 「情報ネットワーク運営者」の主な義務

① 国の定めるネットワークネットセキュリティ等級制度に従い、セキュリティ責任者を置き、セキュリティに関する各種措置を実施する義務（21条）

② （ネットワーク製品やサービスを提供する場合には）提供した製品やサービスが、強制性を有する国家標準に適合しなければならず、不備・欠陥等のリスクが存在するときは、ユーザーおよび関連主管部門に報告する義務（22条）

③ 一部のサービス（インターネット接続、固定電話、モバイル電話等のインターネット接続関連のサービス等）を提供する者は、ユーザーと契約を締結する等の場合に、ユーザーに対して真正な個人情報の提供を要求する義務（24条）

④ ネットワークセキュリティに関する緊急対応策の制定義務（25条）

⑤ 公安機関、国家安全機関が国家安全を維持する活動を行う場合や犯罪捜査を行う場合に、技術サポートおよびその他の協力を提供する義務（28条）

⑥ 国家網信部門および関連部門が実施する監督検査に協力する義務（49条）

⑦ ユーザー情報の秘密保護義務、情報保護制度の構築義務（40条）

⑧ ユーザーの個人情報を収集・使用する場合には、収集・使用に係る規定を公開し、個人情報の収集・使用の目的、方法および範囲を明示し、個人情報の主体の同意を取得する義務（41条）

⑨ 収集した個人情報を漏えい、改ざん、破損してはならず、また、被収集者の同意を得ずに第三者に個人情報を提供してはならない義務（個人が特定できない形での第三者提供を除く）（42条）

# 3. サイバーセキュリティ法
# (2) 情報ネットワーク運営者の義務

①国の定めるネットワークネットセキュリティ等級制度に従い、セキュリティ責任者を置き、セキュリティに関する各種措置を実施する義務（21条）

1. 組織内の安全管理制度及び運営規程を制定し、サイバーセキュリティ責任者を確定し、サイバーセキュリティの保護に係る責任の所在を明確にする。
2. コンピューターウイルス及びサイバー攻撃、ネットワークへの不正侵入等サイバーセキュリティを脅かす行為を防止するための技術的措置を講じる。
3. ネットワークの運用状態、サイバーセキュリティの事件を監視し、規定に従って、少なくとも6か月間、関連するログファイルを保存する。
4. データの分類、重要データのバックアップ及び暗号化等の措置を講じる。
5. 法律、行政法規が定めるその他義務を履行する。

# 3. サイバーセキュリティ法
# (2) 情報ネットワーク運営者の義務

- **「サイバーセキュリティ等級保護制度」（2019年12月1日～）**
  Multi-Level Protection Scheme（MLPS 2.0）
  - **以下に従って**ネットワーク等級**を分ける（15条）**

| 客体 | 損害の程度 | | |
|---|---|---|---|
| | 一般的な損害 | 重大な損害 | 特に重大な損害 |
| 公民、法人その他の組織の合法的な権益 | 1級（低い） | 2級 | 3級 |
| 社会秩序、公共の利益 | 2級 | 3級 | 4級 |
| 国家安全 | 3級 | 4級 | 5級（高い） |

  - **第2級以上のネットワークについては、運営者は専門家による評価・審査を行わなければならず（17条）、公安機関で登録手続（18条）**
  - **第3級以上のネットワークについては、国外からの遠隔地操作による保守点検は原則として禁止（29条。罰則（64条)あり）**

（条文はいずれも条例の意見募集稿による）

# 3. サイバーセキュリティ法
# (2) 情報ネットワーク運営者の義務

- **一般セキュリティ保護義務（20条）･･･全てのネットワーク運営者対象**
  1. サイバーセキュリティー等級保護業務の責任者を決定し、サイバーセキュリティー等級保護業務責任制を確立して、責任追及制度を実行する。
  2. 安全管理および技術保護制度は、人員管理、教育・研修、システムセキュリティー構築、維持管理等の制度を確立する。
  3. 機械室の安全管理、設備、媒体の安全管理、サイバーセキュリティー管理等の制度を実行し、作業規範および作業工程を定める。
  4. 身分識別、悪意のあるコードによる感染の拡散防止、サイバー攻撃防止に対する管理、技術的措置を講じる。
  5. モニタリング、ネットワークの運用状態の記録、サイバーセキュリティー・インシデント、違法・犯罪活動に対する管理および技術的措置を実行し、規定に基づき6カ月以上遡ることのできるネットワーク違法・犯罪に関するログを保存する。
  6. データ分類、重要データのバックアップ、暗号化等の措置を実行する。
  7. 法に基づき個人情報を収集、利用、処理し、個人情報に対する保護措置を実行し、個人情報の漏えい、毀損、改ざん、窃取、滅失、濫用を防止する。
  8. 違法情報の発見、遮断、削除等の措置を実行し、違法情報の大量拡散、違法・犯罪の証拠隠滅等を防止する措置を実行する。
  9. ネットワーク接続の登録およびユーザーの本人確認等の責任を適切に果たす。
  10. ネットワークで発生した案件・事件に対しては、24時間以内に当地の公安機関に報告しなければならない。国家機密を漏えいした場合は、併せてその地の秘密保護行政管理部門に報告しなければならない。
  11. 法律、行政法規で定めるその他のサイバーセキュリティー保護義務

# 3. サイバーセキュリティ法
# (2) 情報ネットワーク運営者の義務

- **自主検査業務（25条）**

  ネットワーク運営者は、当組織のサイバーセキュリティー等級保護制度の実施状況とサイバーセキュリティー状況に対し、毎年少なくとも1度自主検査を実施し、セキュリティー上の潜在的なリスクを発見した場合には速やかに改善し、登録している公安機関に報告しなければならない。

- **データおよび情報のセキュリティ保護（31条）**

  ネットワーク運営者は、重要データおよび個人情報のセキュリティー保護制度を構築し、実行に移し、保護措置を講じて、データおよび情報の収集、保管、伝送、利用、提供、廃棄の過程における安全を保障し、遠隔地でのバックアップ・復旧等の技術的措置を確立して、重要データの完全性、機密性および可用性を保障しなければならない。ネットワーク運営者は、許可または授権を経ずに、その提供するサービスと関係のないデータおよび個人情報を収集してはならない。法律、行政法規の規定および双方の取り決めに違反して、データおよび個人情報を収集、利用、処理してはならない。収集したデータおよび個人情報を漏えい、改ざん、毀損してはならない。授権を受けずにデータおよび個人情報へのアクセス、利用、提供を行ってはならない。

- **罰則（63条）**

  20条、25条、31条などは、CS法59条1項の規定により処罰する。

# 3. サイバーセキュリティ法
# (2) 情報ネットワーク運営者の義務

## ④ネットワークセキュリティに関する緊急対応策の制定義務（25条）

1. ネットワーク運営者は、**サイバーセキュリティ事件緊急対応策を制定**し、システムの脆弱性、コンピューターウイルス、ネットワークへの不正侵入、サイバー攻撃等のセキュリティリスクに速やかに対処しなければならない。
2. サイバーセキュリティを脅かす**事件が発生**した場合は、直ちに緊急対応策を発動し、対応する救済措置を講じるとともに、規定に従って関連の**主管部門に報告**しなければならない。

# 3. サイバーセキュリティ法
# (2) 情報ネットワーク運営者の義務

## ■ 個人情報についての規制（⑧・⑨等）

### ➢ 収集・利用の際の規制（41条）

- 合法、正当、必要の原則を遵守
- 収集・利用に係るルールを公開
- 収集・使用の目的、方法および範囲を明示し、本人の同意を取得
- 提供するサービスに関係のない個人情報を収集してはならない
- 法律、行政法規の規定及び双方間の取決めに違反して、個人情報を収集、使用してはならない
- 法律、行政法規の規定及びユーザーとの取決めに従い、その保存する個人情報を処理しなければならない
- 窃盗又はその他不法な方法により個人情報を取得してはならない（44条）

### ➢ 第三者提供の規制（42条）

- 本人の同意を得ずに第三者に個人情報を提供してはならない義務（個人が特定できない形での第三者提供を除く）

# 3. サイバーセキュリティ法
# (2) 情報ネットワーク運営者の義務

- **管理の規制（42条）**
  - 収集した個人情報を漏えい、改ざん、破損してはならない。
  - 技術的措置及びその他必要な措置を講じ、その収集した個人情報の安全を確保し、情報の漏えい、破損、紛失を防止しなければならない。
- **情報漏えい時の対応（42条）**
  - 個人情報の漏えい、破損、紛失が発生した又は発生する恐れがある場合は、直ちに救済措置を講じ、規定に従って速やかにユーザーに告知するとともに、関連の主管部門に報告しなければならない。
- **削除・訂正権（43条）**
  - ネットワーク運営者が法律、行政法規の規定又は双方間の取決めに違反して、その個人情報を収集、使用していることを発見した場合、ネットワーク運営者にその個人情報の削除を要求する権利を有する。
  - ネットワーク運営者が収集、保存したその個人情報に誤りがあることを発見した場合は、ネットワーク運営者に訂正を要求する権利を有する。
- **苦情の処理（49条）**
  - ネットワーク情報の安全に関する苦情・通報プラットフォームを構築し、苦情・通報方式等の情報を公布し、ネットワーク情報の安全に関する苦情及び通報を速やかに受理、処理しなければならない。

# 3. サイバーセキュリティ法
# (3) 重要情報インフラ運営者の上乗せ義務

## ■ 「重要情報インフラ運営者」の場合

### ➢ 「重要情報インフラ」とは（重要情報インフラ安全保護条例）

この規制でいう重要情報インフラとは、公共の通信・情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政府、国防科学技術産業その他の重要な産業分野、その他の重要なネットワーク設備や情報システムであって、それらが損傷したり、機能を失ったり、データが流出したりすると、国家安全保障、国民生活、公共の利益に重大な危険を及ぼす可能性があるものをいう。

### ➢ 「重要情報インフラ運営者」の場合に追加される主な義務

① 専門のセキュリティ管理機構およびセキュリティ責任者を設置し、定期的に従業員に対する研修をし、重要システム・データのバックアップを実施し、ネットワークセキュリティに関する緊急時の対応策を制定等する義務（34条）

② ネットワーク製品・サービスを購入し、国家の安全に影響を与える可能性がある場合、国家安全審査を受ける義務（35条）

③ ネットワーク製品・サービスを購入する場合、関連規定に従い、提供者との間に安全秘密保持契約を締結し、安全および秘密保持の義務・責任を明確にする義務（36条）

④ **中国で収集したまたは生じた個人情報および重要データは、中国国内で保存する必要があり、業務上の必要性で国外に提供する必要がある場合、CAC・国務院が別途制定する法令に基づき安全評価を受ける義務（37条）**

⑤ 少なくとも1年に一度、ネットワークの安全性およびリスクに関して検査を行い、検査状況を関連部門に送付する義務（38条）

# 3. サイバーセキュリティ法
# (4)ネットワーク製品・サービス提供者の義務

## ■ 「ネットワーク製品・サービス提供者」の場合の義務

① ネットワーク製品・サービスは、関連の国家規格の強制的な要求事項に適合しなければならない

② ネットワーク製品・サービスの提供者は、悪意のあるプログラムを設置してはならない

③ そのネットワーク製品・サービスに安全上の欠陥、脆弱性等のリスクが存在することを発見した場合は、直ちに救済措置を講じ、規定に従って速やかにユーザーに告知し、関連の主管部門に報告しなければならない

④ ネットワーク製品・サービスの提供者は、その製品・サービスにセキュリティメンテナンスを継続的に提供しなければならない。規定された又は当事者が取り決めた期間内に、セキュリティメンテナンスの提供を終了してはならない

⑤ ネットワーク製品・サービスがユーザー情報を収集する機能を有する場合、その提供者は、それをユーザーに明示するとともに同意を得なければならない

⑥ ユーザーの個人情報にかかわる場合、さらに本法及び関連の法律、行政法規における個人情報の保護に関する規定を遵守しなければならない

※ネットワーク製品・サービス安全評価弁法（2017年6月1日施行）

※ネットワーク製品・サービスの安全要件（案）

## ■ 電子情報送信サービス、ソフトのダウンロードサービス

① 安全管理義務を履行

② ユーザーが悪意のあるプログラムを設置したことを知った場合、サービス提供を停止し、除去等の処理・措置を講じ、関連の記録を保存するとともに、関連の主管部門に報告

# 3. サイバーセキュリティ法
# (5) 制裁

## ■ 制裁

➢ **ネットワーク運営者・重要情報インフラ運営者の義務違反などには、行政措置が科せられる（警告、是正命令、業務中止命令、営業許可取消、違法所得没収等）。また制裁金も科せられることがある。**

**（例）**

- **個人情報の収集・利用違反（22条3項、41～43条）**

  →是正命令、情状に基づき警告、違法所得の没収、違法所得の1倍～10倍の過料を単科又は併科。違法所得がない場合は100万元以下の過料。
  直接責任を負う主管者及びその他直接の責任者に対しても1万元以上10万元以下の過料を科すことができる。
  情状が重大な場合、さらに関連業務の一時停止を命じ、営業停止・粛正、ウェブサイトの閉鎖、関連の業務許可の取消し又は営業許可の取消しを行うことができる。

- **個人情報・重要データの国内保存・国外移転のための安全評価（37条）**

  →是正命令、警告を行い、違法所得を没収し、5万元以上50万元以下の過料を科し、関連業務の一時停止、営業停止・粛正、ウェブサイトの閉鎖、関連の業務許可の取消し又は営業許可の取消しを命じることができる。直接責任を負う主管者及びその他直接の責任者に対しては、1万元～10万元の過料。

# 3. サイバーセキュリティ法
# (5) 制裁

- **サイバーセキュリティ保護義務（59条）**

  →ネットワーク運営者（21条、25条違反）

  関連の主管部門が是正を命じ、警告を行う。是正を拒絶した又はサイバーセキュリティを脅かす等の結果をもたらした場合は、1万元以上10万元以下の過料を科する。直接責任を負う主管者に対しては、5,000元以上5万元以下の過料を科する。

  →重要情報インフラの運営者（33条、34条、36条、38条違反）

  関連の主管部門が是正を命じ、警告を行う。是正を拒絶した又はサイバーセキュリティを脅かす等の結果をもたらした場合は、10万元以上100万元以下の過料を科する。直接責任を負う主管者に対しては、1万元以上10万元以下の過料を科する。

- **民事責任（74条1項）**
  - 本法の規定に違反して、他人に損害を与えた場合は、法により民事責任を負う。

# 4. データセキュリティ法

## ■ 事業者の義務（第4章）

- データセキュリティ管理に関する体制整備（27条）
- データセキュリティ教育、訓練の実施（27条）
- 等級保護制度に基づいたデータセキュリティの確保（27条）
- データに関するリスクモニタリング（29条）
- データ・セキュリティ・インシデント対応（29条）
- 規則に従った定期的なリスク評価と当局への提出（重要データ）　（30条）
- データの越境移転のセキュリティ（31条）
- データの合法的かつ正当な取得（32条）

第31条　中華人民共和国の領土内の重要情報インフラストラクチャーの運営者によって収集及び生成された重要なデータの越境セキュリティ管理は、中華人民共和国のサイバーセキュリティ法の規定に準拠するものとする。他のデータ処理者は中華人民共和国国内業務で収集及び生成された重要なデータの越境セキュリティ管理措置は、中国国務院の関連部門と協力して中国国家サイバースペース管理局によって策定されるものとする。

# 4. データセキュリティ法

## ■ ネットワークセキュリティ審査弁法

### ➢ 本弁法に基づきネットワークセキュリティ審査を行う義務（2条）

①**重要情報インフラ事業者がネットワーク製品・サービスを調達する場合**
②ネットワーク・プラットフォーム事業者が国家安全保障に影響を与える、または影響を与える可能性のあるデータ処理活動を行う場合

### ➢ 審査における評価の重点（10条）

①製品及びサービスの使用によってもたらされる重要な情報インフラの不正な制御、妨害または損害のリスク、②製品やサービスの供給の途絶から生じる重要な情報インフラの事業継続性への危険性、③製品及びサービスの安全性、公開性、透明性、ソースの多様性、供給ルートの信頼性、及び政治的、外交的、貿易的、その他の要因による供給途絶の危険性、④製品およびサービス提供者による中国の法律、行政規則、部門規則の遵守、⑤コアデータ、重要データ、大量の個人情報の盗難、漏洩、破壊、不正使用、不正越境のリスク、⑥リストアップされた重要な情報インフラ、コアデータ、重要なデータ、または大量の個人情報が、外国政府によって影響を受け、コントロールされ、または悪意を持って使用されるリスク、およびネットワーク情報セキュリティのリスク、⑦重要な情報インフラのセキュリティ、ネットワークセキュリティ、データセキュリティを危険にさらす可能性のあるその他の要因

### ➢ 協力義務（15条）

「ネットワークセキュリティ審査室が追加資料を要求する場合、当事者、**製品およびサービス提供者は協力するものとする**」

# 4. データセキュリティ法

## ■ 制裁

（例）

➢ **重要データ移転時の安全評価**（31条）の実施違反（46条）

通常の場合

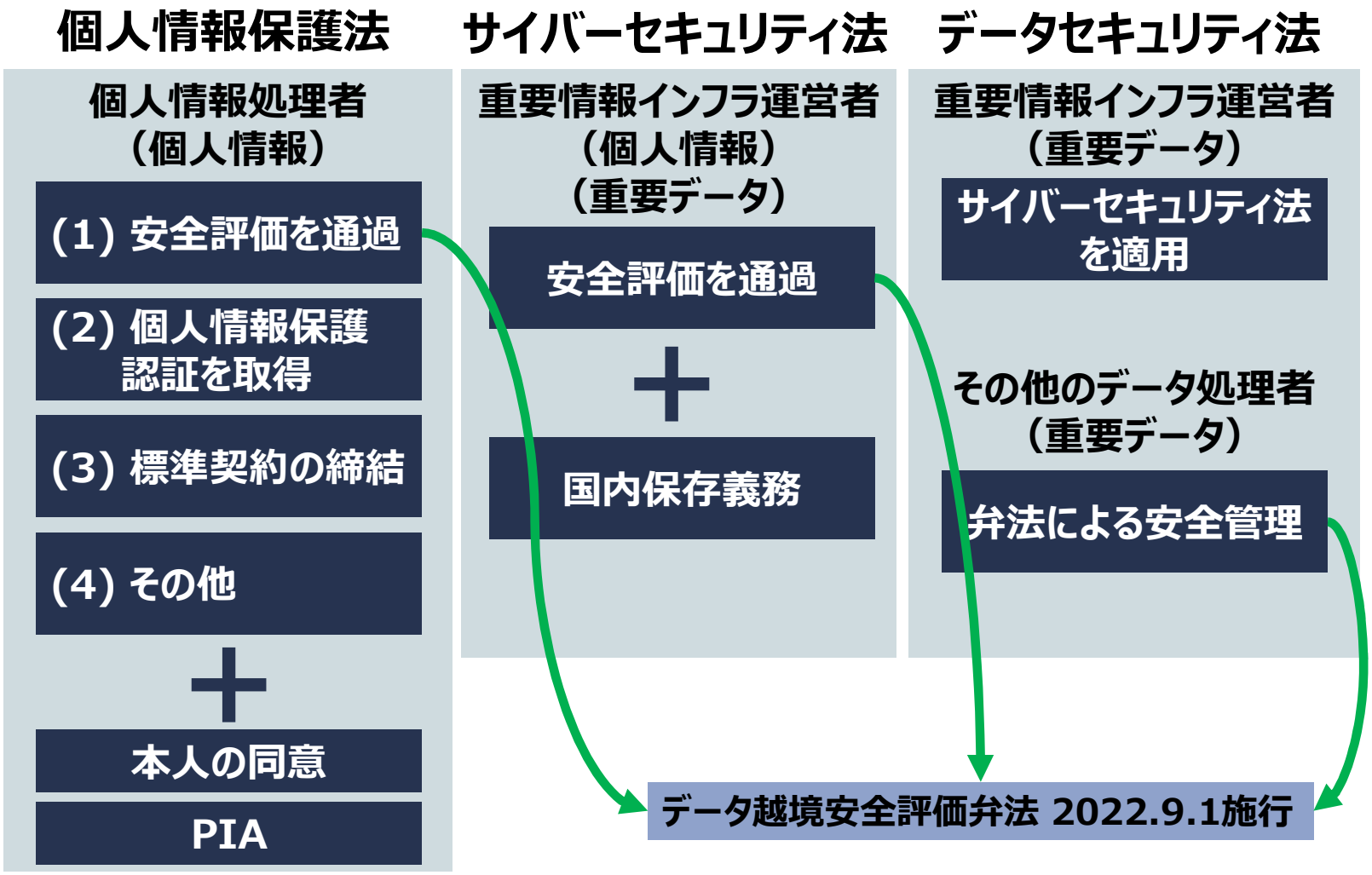
- （会社）10万元以上100万元以下の罰金
- （責任者）1万元以上10万元以下

事態が深刻な場合

- （会社）100万元以上1000万元以下の罰金、及び**関連業務の一時停止、業務の廃止、関連業務許可の取消し、又は営業許可の取消し**
- （責任者）10万元以上100万円以下の罰金

# 目次

# 1. 国外移転規制の全体像



# 2. データ越境安全評価

**個人情報処理者**
**（個人情報）**

- **(1) 安全評価を通過**
- **(2) 個人情報保護認証を取得**
- **(3) 標準契約の締結**
- **(4) その他**

＋

- **本人の同意**
- **PIA**

## データ越境安全評価弁法 2022.9.1施行

以下の場合安全評価の申告が義務（2年ごと更新）

1. 重要データ※1の国外移転
2. 重要情報インフラ運営者 or 100万人以上の個人情報を取扱うデータ処理事業者が個人情報を国外移転
3. 前年1月1日以降に、合計10万人分の個人情報又は1万人分の機微な個人情報※2を国外移転したデータ処理事業者が、国外移転
4. その他国家ネットワーク情報部門が規定する場合

データ移転契約の項目も規定されている

※1 重要データ目録（データセキュリティ法）は未制定
→「情報セキュリティ技術　重要データ識別ガイドライン」及び「国外移転安全評価指針」のパブコメ案あり
※2 GB/T 35273-2020に列挙されている

## 個人情報越境標準契約規定（中国版SCC）2023.6.1施行

# 2. データ越境安全評価

## ■ 「データ越境安全評価弁法」（2022年9月1日施行）

- **手続**

  ①企業が、省級のインターネット情報部門に申告書類を提出（弁法6条）

  ②国家インターネット情報部門が安全評価（同7条、11条）

  - **評価の有効期間**

    2年間。有効期間満了の60営業日前に再申告が必要

- **提出書類（データ越境セキュリティ評価報告書作成手引き）**

  1.統一社会信用規約文書の写し

  2.法定代理人の身分証明書の写し

  3.担当者の身分証明書の写し

  4.管理者の承認書（附属書2）

  5.データ越境セキュリティ評価宣言（附属書3）

  6.海外の受取人との越境契約書等の法的拘束力のある文書の写し

  7.データ越境リスクに関する自己評価報告書（附属書4）→ひな形

  8.その他関連する補足資料

  ※要中国語

  - **「データ国外移転安全評価指針（第2草案）」があったが未施行**

# 3. 個人情報保護認証

## ■ 「個人情報保護認証実施規則」（2022年11月4日）

### １．認証の要件

**越境移転を行う個人情報処理者はTC260-PG-20222A（個人情報越境処理活動安全認証規則）の要求事項（最新版）を遵守しなければならない。**

※個人情報越境処理活動安全認証規則については、現時点で第二版が公表されている。

### ２．認証までのフロー

**①個人情報処理者に認証機関に対する認証委託（具体的には資料提出等）**
**②技術検証**
**③現地審査**
**④認証決定・認証証明書の発行**

### ３．認証後の監督及び有効期限

**認証証明書の有効期限は3年間であるが、個人情報処理者は、有効期間中、認証機関の継続的な監督に服し、認証の有効性を維持しなければならない。認証の更新が必要な場合、個人情報処理者は、失効日の6ヶ月前以内に認証委託を行わなければならない。**

# 4. 個人情報越境移転標準契約（中国版SCC）

## ■ 「個人情報越境標準契約弁法」（2023年2月24日公布）

- **2023年6月1日施行**
- **是正期間は2023年11月30日まで**

- **発効日から10営業日以内に所在地の省級のインターネット情報部門に届出をする義務**

- **提出書類（個人情報越境についての標準契約届出手引き（2023年5月30日））**
  1. 統一社会信用コード証書の写し
  2. 法定代表者身分証明書の写し
  3. 担当者の身分証明書の写し
  4. 担当者の授権委任状（付属書類2）
  5. 承諾書（付属書類3）
  6. 標準契約（付属書類4）
  7. 「個人情報保護影響評価報告書」（PIA）（付属書類5）

- **15営業日以内に書類の検査を完了し、「通過」「不通過」の通知が行われる**

# 5. 個人情報保護影響評価（PIA）

## ■ 位置づけ

- **個人情報を中国国外に提供する場合にはPIAが義務（PIPL55条）**
- **個人情報越境移転標準契約の届出の際に「PIA報告書」提出義務**

## ■ 何をするのか？

- **評価項目（PIPL56条1項）**
  1. 個人情報の処理目的及び処理方法が合法であり、適切かつ必要であるかどうか
  2. 個人の権利とセキュリティリスクへの影響
  3. 採用された保護措置が合法であり、効果的であり、リスクの程度に適合しているかどうか
- **評価項目（重点項目。越境移転標準契約5条の義務）**
  1. 個人情報処理者及び国外受領者が個人情報の処理を行う目的、範囲、方法等の適法性、正当性、必要性
  2. 越境する個人情報の規模、範囲、種類、機微の度合い、個人情報の越境が個人情報の権利利益にもたらす可能性のあるリスク
  3. 国外受領者が負う義務、義務を履行する管理的及び技術的措置、越境する個人情報の安全を保障する能力
  4. 個人情報の越境後の改ざん、破壊、漏えい、紛失、不法な利用等のリスク、個人情報の権利利益を保護する方法が円滑であるか等
  5. 国外受領者の所在国又は地域の個人情報保護政策及び法規が標準契約の履行に及ぼす影響
  6. 個人情報の越境の安全性に影響を及ぼす可能性のあるその他の事項

# 5. 個人情報保護影響評価（PIA）

**「個人情報越境についての標準契約届出手引き」付属書5には、以下の記載あり**

三、越境活動の影響評価に関する状況

次の各号に基づき逐次に影響評価の状況を説明し、発見された問題やリスク及びそれに対応する改善策や効果を巡って重点的に説明すること。

（1）個人情報処理者と受取者が個人情報を処理する目的、範囲、方法などの合法性、正当性、必要性。

（2）越境する個人情報の規模、範囲、種類、敏感度、個人情報の越境によって発生しうる個人情報の権益に関するリスク。

（3）域外受取者が背負うと承諾する義務、及びその義務を履行するための管理・技術措置、能力等は越境する個人情報の安全を保障できるかどうか。

（4）個人情報が越境した後に、改ざん、破壊、漏洩、紛失、不正利用などのリスク、個人情報の権益を保護するためのチャネルに障害があるかどうか。

（5）域外受取者の国または地域の個人情報保護の政策と法令が標準契約の履行に与える影響。

（6）その他、個人情報の越境安全に影響を及ぼす可能性のある事項。

四、越境活動の影響評価の結論

上記の影響評価の状況と相応する改善状況を総合的に考慮し、客観的な影響評価の結論を導き出し、その理由と根拠を十分に説明すること。

**越境活動についての評価のみを提出すれば良いことが分かって一安心**

**しかしながら、肝心の「影響評価」の方法については記載がない**

# 5. 個人情報保護影響評価（PIA）

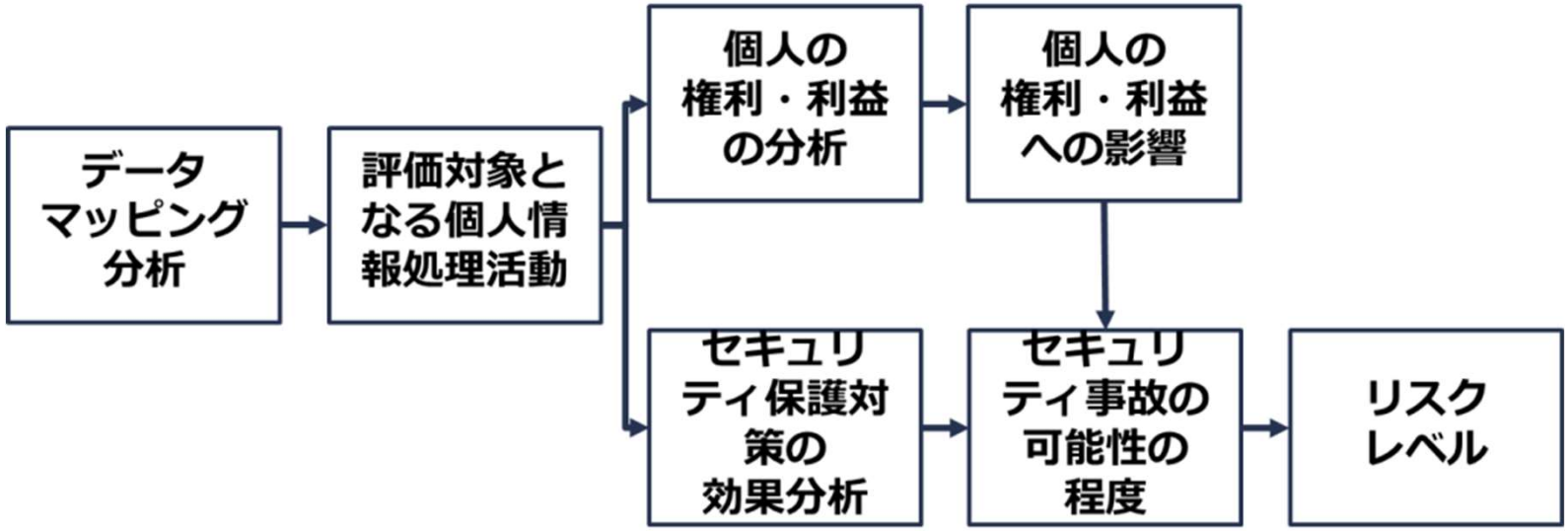
## ■ 具体的な手法

- **概要：「情報安全技術 個人情報安全規範」（GB/T 35273-2020）11.4**
- **方法：「個人情報セキュリティ影響評価ガイドライン」（GB/T 39335-2020）**
  - リファレンスとして「ISO/IEC FDIS 29134:2017 Information technology – Security techniques -Privacy impact assessment」を挙げている
    →Privacy Impact Assessment（PIA）の一般的な手法に従った手順や内容
  - ISO/IEC FDIS 29134:2017を日本語化したものが「JISX 9251：2021（情報技術－セキュリティ技術－プライバシー影響評価のためのガイドライン）」
  - 個人情報保護委員会が、JISX 9251：2021を参考にしつつ、「PIAの取組の促進について-PIAの意義と実施手順に沿った留意点-」を公表

- **PIAの最初のプロセスとして必要となるデータマッピングの意味や方法論**
  **→個人情報保護委員会が「データマッピングツールキット」**

# 5. 個人情報保護影響評価（PIA）

- 「個人情報セキュリティ影響評価ガイドライン」の手順




- ただし、実務的には、処理活動全体に対するPIAは別途対応することとし、越境移転のPIAを「TIA（Transfer Impact Assessment）」と似た発想で行って当局への届出を済ませることもあり得る

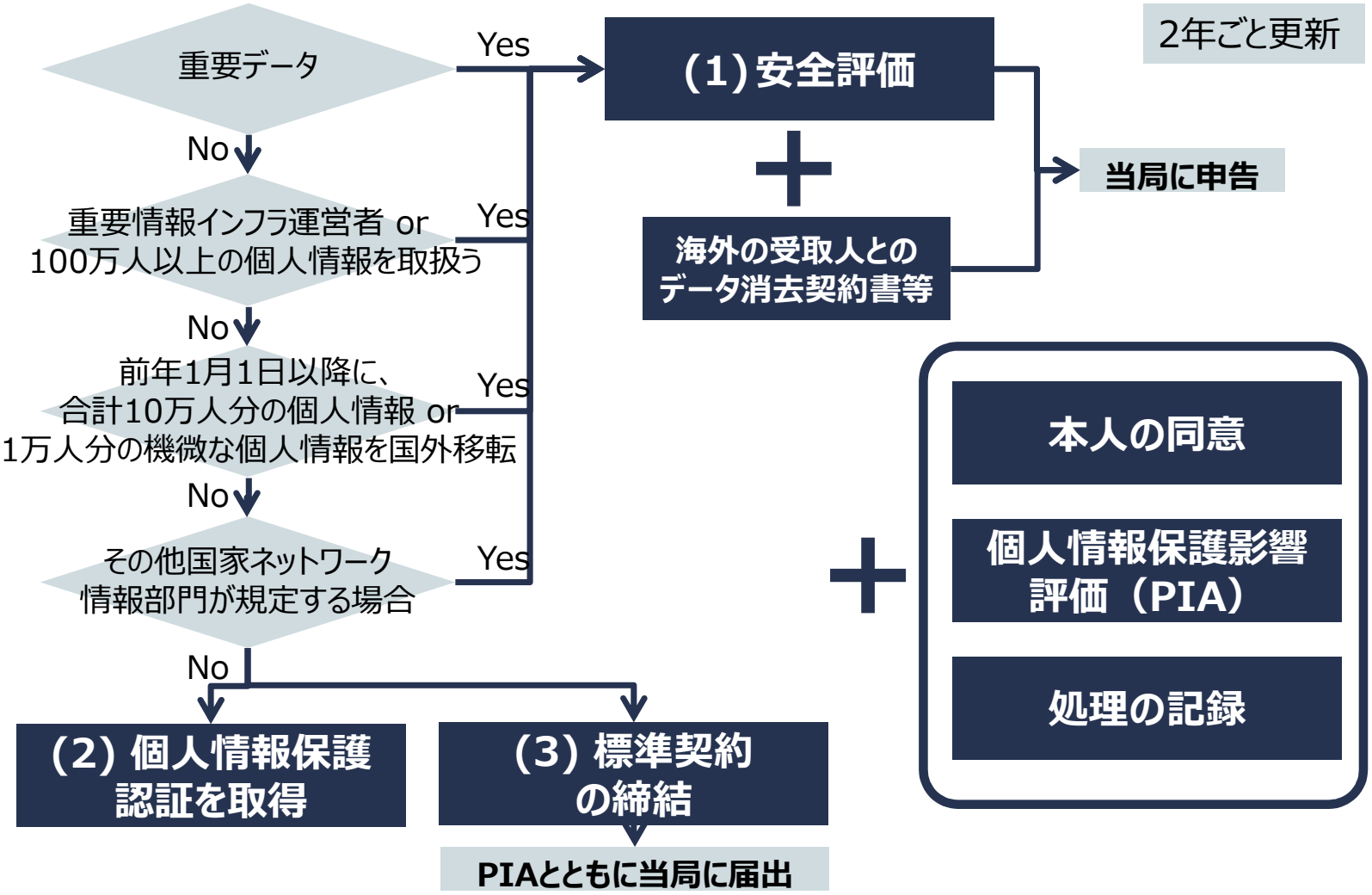
# 6. 処理活動の記録

## ■ 処理活動の記録

- **個人情報保護法55条**
  **個人情報を国外移転する場合には、「事前に個人情報保護影響評価を実施し、処理活動を記録するものとする。」**

- **「情報安全技術 個人情報安全規範」（GB/T 35273-2020）11.3**
  - 処理活動の記録には以下を含むことを例示
    a. 対象となる個人情報の種類、量及び出所（例えば、本人から直接収集されたものか間接的に取得されたものか）
    b. 業務機能・権限に応じて個人情報の処理目的及び利用シナリオ、処理の委託・共有・提供・公開及び国外移転が含まれるかの情報の識別
    c. 個人情報の処理活動の各段階において関与する情報システム、組織及び人員
- **これらの項目は、「個人情報セキュリティ影響評価ガイドライン」（GB/T 39335-2020）に基づくPIAで特定する**
  **→データマッピング・シートに記載**
  **→個人情報保護影響評価書（PIA報告書）に含まれる**
  **→これを保管**

# 7. まとめ


重要データ
Yes
No
重要情報インフラ運営者 or
100万人以上の個人情報を取扱う
Yes
No
前年1月1日以降に、
合計10万人分の個人情報 or
1万人分の機微な個人情報を国外移転
Yes
No
その他国家ネットワーク
情報部門が規定する場合
Yes
No
(1) 安全評価
2年ごと更新
海外の受取人との
データ消去契約書等
当局に申告
本人の同意
個人情報保護影響
評価（PIA）
処理の記録
(2) 個人情報保護
認証を取得
(3) 標準契約
の締結
PIAとともに当局に届出

# 目次



# 1. 重要データの越境移転規制の全体像

## ■ 「重要データ」の越境移転規制

### ➢ サイバーセキュリティ法37条

「重要情報インフラ運営者が中華人民共和国国内での運営において収集・生成された個人情報及び重要データは、中国国内で保存しなければならない。業務上の確かな必要により越境移転を行う必要がある場合、国家ネットワーク情報部門が国務院の関連部門と共同して定めた規則に従って安全評価を受けなければならない」

### ➢ データセキュリティ法31条

「重要情報インフラ運営者が中華人民共和国国内の運営中に収集し、発生させた重要データの越境安全管理は、「中華人民共和国サイバーセキュリティ法」の規定を適用する。
その他のデータ処理者が中華人民共和国国内の運営において収集し、発生させた重要データの越境安全管理弁法は、国家インターネット情報通信部門が国務院の関係部門と共同で制定する。」

### ➢ データ越境安全評価弁法4条

「データ処理者は、国外にデータを提供するとき、以下のいずれかに該当する場合、所在地の省級のインターネット情報部門を通じて、国家インターネット情報部門にデータ越境安全評価を申告しなければならない。

(一)データ処理者が重要データを国外に提供する場合。［以下略］

# 1. 重要データの越境移転規制の全体像

| 重要情報インフラ運営者 | 重要データ | 個人情報 | 中国国内への保存 | | 越境移転の際の安全評価 | |
|---|---|---|---|---|---|---|
| ○ | ○ | ○ | ○ | PIPL40条<br>CCSL37条 | ○ | PIPL40条<br>CCSL37条<br>CDSL31条1文 |
| | | × | ○ | CCSL37条 | ○ | CCSL37条<br>CDSL31条1文 |
| ○ | × | ○ | ○ | PIPL40条<br>CCSL37条 | ○ | PIPL40条<br>CCSL37条 |
| | | × | × | | × | |
| × | ○ | ○ | △ | PIPL40条<br>(一定の数量) | ○ | PIPL40条<br>CDSL31条2文<br>安評弁4条1号 |
| | | × | × | | ○ | CDSL31条2文<br>安評弁4条1号 |
| × | × | ○ | △ | PIPL40条<br>(一定の数量) | △ | PIPL40条<br>安評弁4条2,3号 |
| | | × | × | | × | |

# 2. 重要データとは？

## ■ 何が「重要データ」に当たるのか？

### ➢ データ越境移転安全評価弁法19条

「本弁法にいう重要データとは、いったん改ざん、破壊、漏えい又は不正取得、不正利用等が生じた場合に国の安全、経済運営、社会の安定、公衆衛生及び安全に危害を及ぼすおそれのあるデータをいう」

→「重要データ」の定義及び範囲は明確ではない

### ➢ データセキュリティ法21条3項

「各地域、各部門はデータ分類・分級保護制度に基づき、本地域、本部門及び関連業界・分野の重要データの具体的な分類目録を確定しなければならない」

### ➢ サイバーセキュリティ標準実践ガイドライン――インターネットデータの分類と分級に関する指針」（TC260-PG-20212A）

- 一般データ、重要データ、核心データの3つのレベルに分類

# 2. 重要データとは？

- **「情報セキュリティ技術　重要データ識別ガイドライン」案（2022年1月13日～パブコメ）**
  → 「重要データ目録」 *を定めるとしている

*かつて「データ国外移転安全評価指針（第1草案）」では27の分野毎に重要データに該当するものが列挙されていた

**第5項は、以下が重要データであると定める**

重要なデータを特定する場合、以下の要素を考慮することができる。

a. 戦略物資の生産能力や備蓄など、国家戦略的備蓄や緊急動員能力を反映したものが重要なデータである。

b. 重要インフラの運用や重要地域の産業生産を支援するもので、重要インフラが位置する産業や分野の中核事業の運用や重要地域の産業生産を直接支援するデータが重要なデータである。

c. 重要情報インフラのネットワークセキュリティ保護を反映したもので、重要情報インフラに対するサイバー攻撃の実行に利用できるもの。例えば、重要情報インフラのネットワークセキュリティ計画を反映したデータ、システム構成情報、コアソフトウェアおよびハードウェア設計情報、システムトポロジー、緊急時計画等が重要なデータである。

d. 輸出管理品目に関するデータであって、輸出管理品目の設計原理、プロセスフロー、製造方法等を記述した情報、ソースコード、集積回路レイアウト図、技術計画、重要パラメータ、実験データ、テストレポート等が重要なデータである。

e. 地理情報であって、一定の精度要件を満たすもの等、他の国や組織が中国に対して軍事攻撃を行うために利用する可能性があるデータが重要なデータとなる。

f. テロリストや犯罪者が損害を与えるために使用する可能性のある重要目標、重要拠点、非公開の地理的目標の位置の物理的安全保護を反映したデータ、例えば、重要保安単位、重要生産企業、重要国家資産（鉄道、石油パイプラインなど）の建設計画、内部構造、セキュリティなどの情報、非公開の特別道路、非公開の空港に関する情報などは重要である。

# 2. 重要データとは？

g. 重要な顧客のリスト、重要な情報基盤事業者による製品・サービスの調達に関する未公開情報、未公開の重要な脆弱性など、重要な機器やシステム部品のサプライチェーンに障害を与え、高度持続的脅威などのサイバー攻撃を仕掛けるために悪用される可能性があるデータは、重要なデータである。

h. 集団における健康状態、生理状態、民族的特徴、遺伝情報等を反映した基本データ、例えば、人口調査情報、ヒト遺伝資源情報、遺伝子配列の生データは重要なデータである。

i. 国の天然資源および環境に関する基本データ。例えば、水の状態に関する未発表の情報、水文観測、気象観測、環境モニタリングデータなどは重要なデータである。

j. 国防や国家安全保障に関連する知的財産権を記述したデータなど、科学技術力に関連し、国際競争力に影響を与えるデタは重要なデータである。

k. 重要企業の金融取引に関するデータ、重要機器の生産・製造に関する情報、国家的な主要プロジェクトの建設やその他の生産活動における重要機器の装備・使用に関する情報など、外国政府から制裁を受ける可能性のある機密項目の生産・取引および重要機器の装備・使用に関するデータは重要なデータである。

l. 政府機関、軍需企業、その他の機密かつ重要な機関にサービスを提供する過程で発生する情報で、軍需企業による長期間の車両使用に関する情報など、一般公開には適さない情報。

m. 未公開の統計データなど、未公開の政府データ、業務秘密、情報データおよび法執行・司法データ

n. その他、国家の政治、領土、軍事、経済、文化、社会、科学技術、生態、資源、核施設、海外利益、生物、宇宙、極、深海などの安全に影響を与える可能性があるデータ。

**上記のうち1つでも該当するものは重要なデータである。**

# 2. 重要データとは？

- **「自動車データセキュリティ管理若干規定（試行）」（2021年10月1日施行）**

1. 重要センシティブ・エリア（軍事管理エリア、国防科学工業機関および県レベル以上の中国共産党機関・国家行政機関等）の地理情報、歩行者通行量・車両通行量に関するデータ
2. 車両の走行量、物流等の経済状況を反映するデータ
3. 車両充電ネットワークの稼働データ
4. 顔、ナンバープレート情報等を含む車外の撮影、画像データ
5. 10 万人を超える個人情報主体に関わる個人情報
6. 主管機関が確定する国家の安全、公共の利益、個人や組織の合法的権益に危害を及ぼす可能性があるデータ

- **「工業及び情報化分野のデータセキュリティ管理弁法（試行）」案（2022年2月10日～パブコメ）**

危害の程度が次のいずれかに該当するデータは、重要データに当たる。

1. 政治、領土、軍事、経済、文化、社会、科学技術、電磁、ネットワーク、生態、資源、原子力安全等に脅威を与え、中国の国外の利益、生物、宇宙、極地、深海、人工知能その他の国家安全保障に関連する重要分野に影響を及ぼす
2. 産業および情報技術の分野における開発、生産、運営および経済的利益に重大な影響を与える
3. 重大なデータセキュリティ事故または生産安全事故を引き起こし、公共の利益または個人もしくは団体の正当な権利および利益に重大な影響を与え、社会的に大きな負の影響を与える
4. 明らかな連鎖的影響を引き起こし、影響範囲が複数の業界、地域、または業界の複数の企業に及び、または影響が長期間続き、業界の発展、技術進歩、産業生態などに深刻な影響を与える
5. 工業情報化部門が評価・決定したその他の重要なデータ

# 2. 重要データとは？

- **「ネットワークデータセキュリティ管理条例」案（2021年11月14日～パブコメ）**

1. 非公開の政府データ、仕事上の秘密、情報データ、法執行機関や司法機関のデータ
2. 輸出管理データ、輸出管理品目に関わるコア技術、設計スキーム、生産プロセスに関するデータ、暗号、生物、電子情報、人工知能など、国家安全保障や経済の競争力に直接影響を与える分野の科学技術成果に関するデータ
3. 国家の経済運営データ、重要産業のビジネスデータ、統計データなどで、国の法律、行政法規、部門規定で保護または普及制御が明確に求められているもの
4. 産業、通信、エネルギー、交通、水利、金融、国防科学技術産業、税関、税務などの主要産業・分野の安全な生産・運営に関するデータ、主要なシステムコンポーネントや機器のサプライチェーンデータ
5. 遺伝子、地理、鉱物、気象データなど、人口や健康、天然資源、環境に関する国家基本データで、国家の関連部門が指定する規模や精度に達しているもの
6. 国家インフラ、重要情報インフラの構築・運用とそのセキュリティデータ、国防施設、軍管理区域、国防研究・生産ユニットなどの重要かつ機密性の高いエリアの地理的位置とセキュリティに関するデータ
7. その他、国家の政治、領土、軍事、経済、文化、社会、科学技術、生態、資源、核施設、海外の利益、生物、宇宙、極地、深海などの安全に影響を与える可能性のあるデータ

# 3. 実務対応のモック

## ■ 非個人情報の「重要データ」に留意

### ➢ ケース：日本企業が中国企業に工作機械を輸出し、当該工作機械の稼働データを日本のサーバで受信する

- **「情報セキュリティ技術　重要データ識別ガイドライン」（パブコメ）**

  「d) 輸出管理品目に関するデータであって、輸出管理品目の設計原理、プロセスフロー、製造方法等を記述した情報、ソースコード、集積回路レイアウト図、技術計画、重要パラメータ、実験データ、テストレポート等」

- **「ネットワークデータセキュリティ管理条例」案」（パブコメ）**

  「輸出管理品目に関わるコア技術、設計スキーム、生産プロセスに関するデータ」

  **中国政府が定める「輸出管理品目」に該当する物品やサービス等に関するデータは、重要データに当たる可能性あり**

- **営業活動の過程で顧客である中国企業から聞いた投資計画や生産計画などが「重要データ」に当たる可能性はないか？**

- **「工業及び情報化分野のデータセキュリティ管理弁法(試行)」(パブコメ)**

  「明らかな連鎖的影響を引き起こし、影響範囲が複数の業界、地域、または業界の複数の企業に及び、または影響が長期間続き、業界の発展、技術進歩、産業生態などに深刻な影響を与える」

# 3. 実務対応のモック

- **「情報セキュリティ技術　重要データ識別ガイドライン」案（2022年1月13日～パブコメ）**
  → 「重要データ目録」*を定めるとしている

  **第5項は、以下が重要データであると定める**

  重要なデータを特定する場合、以下の要素を考慮することができる。

  a. 戦略物資の生産能力や備蓄など、国家戦略的備蓄や緊急動員能力を反映したものが重要なデータである。
  b. 重要インフラの運用や重要地域の産業生産を支援するもので、重要インフラが位置する産業や分野の中核事業の運用や重要地域の産業生産を直接支援するデータが重要なデータである。
  c. 重要情報インフラのネットワークセキュリティ保護を反映したもので、重要情報インフラに対するサイバー攻撃の実行に利用できるもの。例えば、重要情報インフラのネットワークセキュリティ計画を反映したデータ、システム構成情報、コアソフトウェアおよびハードウェア設計情報、システムトポロジー、緊急時計画等が重要なデータである。
  **d. 輸出管理品目に関するデータであって、輸出管理品目の設計原理、プロセスフロー、製造方法等を記述した情報、ソースコード、集積回路レイアウト図、技術計画、重要パラメータ、実験データ、テストレポート等が重要なデータである。**
  **e. 地理情報であって、一定の精度要件を満たすもの等、他の国や組織が中国に対して軍事攻撃を行うために利用する可能性があるデータが重要なデータとなる。**

# 3. 実務対応のモック

f. テロリストや犯罪者が損害を与えるために使用する可能性のある重要目標、重要拠点、非公開の地理的目標の位置の物理的安全保護を反映したデータ、例えば、重要保安単位、重要生産企業、重要国家資産（鉄道、石油パイプラインなど）の建設計画、内部構造、セキュリティなどの情報、非公開の特別道路、非公開の空港に関する情報などは重要である。
g. 重要な顧客のリスト、重要な情報基盤事業者による製品・サービスの調達に関する未公開情報、未公開の重要な脆弱性など、重要な機器やシステム部品のサプライチェーンに障害を与え、高度持続的脅威などのサイバー攻撃を仕掛けるために悪用される可能性があるデータは、重要なデータである。
h. 集団における健康状態、生理状態、民族的特徴、遺伝情報等を反映した基本データ、例えば、人口調査情報、ヒト遺伝資源情報、遺伝子配列の生データは重要なデータである。
i. 国の天然資源および環境に関する基本データ。例えば、水の状態に関する未発表の情報、水文観測、気象観測、環境モニタリングデータなどは重要なデータである。
j. 国防や国家安全保障に関連する知的財産権を記述したデータなど、科学技術力に関連し、国際競争力に影響を与えるデタは重要なデータである。
k. 重要企業の金融取引に関するデータ、重要機器の生産・製造に関する情報、国家的な主要プロジェクトの建設やその他の生産活動における重要機器の装備・使用に関する情報など、外国政府から制裁を受ける可能性のある機密項目の生産・取引および重要機器の装備・使用に関するデータは重要なデータである。
l. 政府機関、軍需企業、その他の機密かつ重要な機関にサービスを提供する過程で発生する情報で、軍需企業による長期間の車両使用に関する情報など、一般公開には適さない情報。
m. 未公開の統計データなど、未公開の政府データ、業務秘密、情報データおよび法執行・司法データ
n. その他、国家の政治、領土、軍事、経済、文化、社会、科学技術、生態、資源、核施設、海外利益、生物、宇宙、極、深海などの安全に影響を与える可能性があるデータ。

上記のうち1つでも該当するものは重要なデータである。

# 3. 実務対応のモック

## ➢ 「自動車データセキュリティ管理若干規定（試行）」（2021年10月1日施行）

1. **重要センシティブ・エリア（軍事管理エリア、国防科学工業機関および県レベル以上の中国共産党機関・国家行政機関等）の地理情報、歩行者通行量・車両通行量に関するデータ**
2. **車両の走行量、物流等の経済状況を反映するデータ**
3. 車両充電ネットワークの稼働データ
4. 顔、ナンバープレート情報等を含む車外の撮影、画像データ
5. 10 万人を超える個人情報主体に関わる個人情報
6. 主管機関が確定する国家の安全、公共の利益、個人や組織の合法的権益に危害を及ぼす可能性があるデータ

## ➢ 「工業及び情報化分野のデータセキュリティ管理弁法（試行）」案（2022年2月10日～パブコメ）

危害の程度が次のいずれかに該当するデータは、重要データに当たる。

1. 政治、領土、軍事、経済、文化、社会、科学技術、電磁、ネットワーク、生態、資源、原子力安全等に脅威を与え、中国の国外の利益、生物、宇宙、極地、深海、人工知能その他の国家安全保障に関連する重要分野に影響を及ぼす
2. 産業および情報技術の分野における開発、生産、運営および経済的利益に重大な影響を与える
3. 重大なデータセキュリティ事故または生産安全事故を引き起こし、公共の利益または個人もしくは団体の正当な権利および利益に重大な影響を与え、社会的に大きな負の影響を与える
4. **明らかな連鎖的影響を引き起こし、影響範囲が複数の業界、地域、または業界の複数の企業に及び、または影響が長期間続き、業界の発展、技術進歩、産業生態などに深刻な影響を与える**
5. 工業情報化部門が評価・決定したその他の重要なデータ

# 3. 実務対応のモック

- **「ネットワークデータセキュリティ管理条例」案**
  **（2021年11月14日～パブコメ）**

1. 非公開の政府データ、仕事上の秘密、情報データ、法執行機関や司法機関のデータ
2. **輸出管理データ、輸出管理品目に関わるコア技術、設計スキーム、生産プロセスに関するデータ、暗号、生物、電子情報、人工知能など、国家安全保障や経済の競争力に直接影響を与える分野の科学技術成果に関するデータ**
3. 国家の経済運営データ、重要産業のビジネスデータ、統計データなどで、国の法律、行政法規、部門規定で保護または普及制御が明確に求められているもの
4. 産業、通信、エネルギー、交通、水利、金融、国防科学技術産業、税関、税務などの主要産業・分野の安全な生産・運営に関するデータ、主要なシステムコンポーネントや機器のサプライチェーンデータ
5. 遺伝子、地理、鉱物、気象データなど、人口や健康、天然資源、環境に関する国家基本データで、国家の関連部門が指定する規模や精度に達しているもの
6. 国家インフラ、重要情報インフラの構築・運用とそのセキュリティデータ、国防施設、軍管理区域、国防研究・生産ユニットなどの重要かつ機密性の高いエリアの地理的位置とセキュリティに関するデータ
7. その他、国家の政治、領土、軍事、経済、文化、社会、科学技術、生態、資源、核施設、海外の利益、生物、宇宙、極地、深海などの安全に影響を与える可能性のあるデータ

# 4. 重要データの越境移転規制の全体像（再掲）

| 重要情報インフラ運営者 | 重要データ | 個人情報 | 中国国内への保存 | | 越境移転の際の安全評価 | |
|---|---|---|---|---|---|---|
| ○ | ○ | ○ | ○ | PIPL40条<br>CCSL37条 | ○ | PIPL40条<br>CCSL37条<br>CDSL31条1文 |
| | | × | ○ | CCSL37条 | ○ | CCSL37条<br>CDSL31条1文 |
| ○ | × | ○ | ○ | PIPL40条<br>CCSL37条 | ○ | PIPL40条<br>CCSL37条 |
| | | × | × | | × | |
| × | ○ | ○ | △ | PIPL40条<br>(一定の数量) | ○ | PIPL40条<br>CDSL31条2文<br>安評弁4条1号 |
| | | × | × | | ○ | CDSL31条2文<br>安評弁4条1号 |
| × | × | ○ | △ | PIPL40条<br>(一定の数量) | △ | PIPL40条<br>安評弁4条2,3号 |
| | | × | × | | × | |