ジェトロ北京　進出企業支援セミナー
中国日本商会・天津日本人会共催

JT&N 金诚同达律师事务所

中国での事業活動における情報の収集・保存・利用の留意点：サイバーセキュリティ法、データセキュリティ法、個人情報保護法と実務対応

北京金誠同達法律事務所
マネジメントパートナー
張　国棟

マネジメントパートナー/弁護士　張 国棟

＜連絡方法＞

Tel:（8610) 5706-8268　　Mobile（Wechat）: (86) 139-1183-3645

Email: zhangguodong@jtnfa.com　　lawyerzhang@hotmail.com

張国棟弁護士は、投資、コンプライアンス、競争法、合併買収・再編、紛争解決などの分野において、二十年の業務経験を既に有しています。政府規制関連の業務において、体系の構築および個別案件への対応を含む総合サービスを提供しており、独占禁止、商業賄賂防止、サイバーセキュリティ、データ保護、税関、外貨、環境保護などの分野においては、いずれも豊富な業務経験を有しています。具体的な業界の面では、張国棟弁護士は、医薬、自動車およびIT分野における特別な監督管理と業界の課題に熟達しており、多くのクライアントに長期的なサービスを提供しています。

張国棟弁護士は、現在では金誠同達法律事務所のマネジメントパートナー、執行副主任を担当しており、北京市弁護士協会競争・独占禁止法律専門委員会の副主任、多くの大学で非常勤指導教官を兼任しています。張国棟弁護士は、チームを率いてALBの主催する「年間日本業務優秀海外法律事務所」の大賞を獲得し、自身も「商法」（China Business Law Journal ）という雑誌において「中国法曹界の傑物」というご評価をいただきました。張国棟弁護士はこれまでにも、数々の国内外の雑誌において論文を発表し、ご招待を受けてフォーラムにて講演を行い、レクシスネクシス社（Lexis Nexis）の法律データベース上にて「律観棟察」と題する法律コラムを開設しています。

CONTENTS

金诚同达律师事务所

一、背景と各法の概要

1.1.1 「サイバーセキュリティ法」

◆国際的な背景

✓国際的なサイバーセキュリティの法的環境には、今まさに変革の最中であり、**サイバーセキュリティ**は既に**グローバルな問題**となっている。

✓**アメリカやEU等**のIT強国では、サイバーセキュリティをめぐる**立法の体系が次々に確立**されている。

✓サイバーセキュリティをめぐる立法は、グローバルな範囲内における利益の調整と国家同士の主権の争いへと変化しており、根拠となり得る法令の存在は、**交渉と対抗の必要条件**となる。

出典：国家インターネット情報弁公室　2016年11月7日

http://www.cac.gov.cn/2016-11/07/c_1119866606.htm

1.1.1 「サイバーセキュリティ法」

◆中国国内における背景

✓2015年には「中華人民共和国**国家安全法**」が**可決**されている。

✓2015年の7月には、サイバーセキュリティの基本法として「サイバーセキュリティ法（草案）」が初めて社会からの意見が募集されている。2016年の11月7日には、全国人民代表大会常務委員会において、「サイバーセキュリティ法」が可決された。

✓立法の迅速な推進は、中国が直面する国内外の**サイバーセキュリティの形勢の客観的な実際の緊迫した必要性**に応じるためのものであり、中国における**サイバー空間の法制化の過程の実質的な展開**を表している。

出典：国家インターネット情報弁公室　2016年11月7日

http://www.cac.gov.cn/2016-11/07/c_1119866606.htm

1.1.2 「データセキュリティ法」、「個人情報保護法」

◆国際的な背景

✓データと個人情報の保護の強化は、国際的な発展の潮流とすう勢に合致している。

【**欧州連合**の2018年の「General Data Protection Regulation」（**GDPR**）】

【**アメリカ合衆国カリフォルニア州**の2018年の「California Consumer Protection Act」（ **CCPA** ）】

【**日本国**の2020年の「**個人情報の保護に関する法律**」改正】

✓国際的な競争、特に、データをめぐる競争が加速されている。

1.1.2 「データセキュリティ法」、「個人情報保護法」

◆中国国内における背景

✓**データセキュリティと個人情報保護の問題**は、モバイルインターネット時代において更に**顕在化**している。

【スマートフォンを通じたスパムの頻発】

【オンライン詐欺者による被害者の家庭住所などを詳細に把握することが可能化】

【新型コロナウィルス患者の個人情報のネットワーク上への流出】

✓従前の規定は**分散**しており、法律の**等級は比較的に低く**、立法上における**空白が存在**していた。

1.2.1 概要と位置づけ

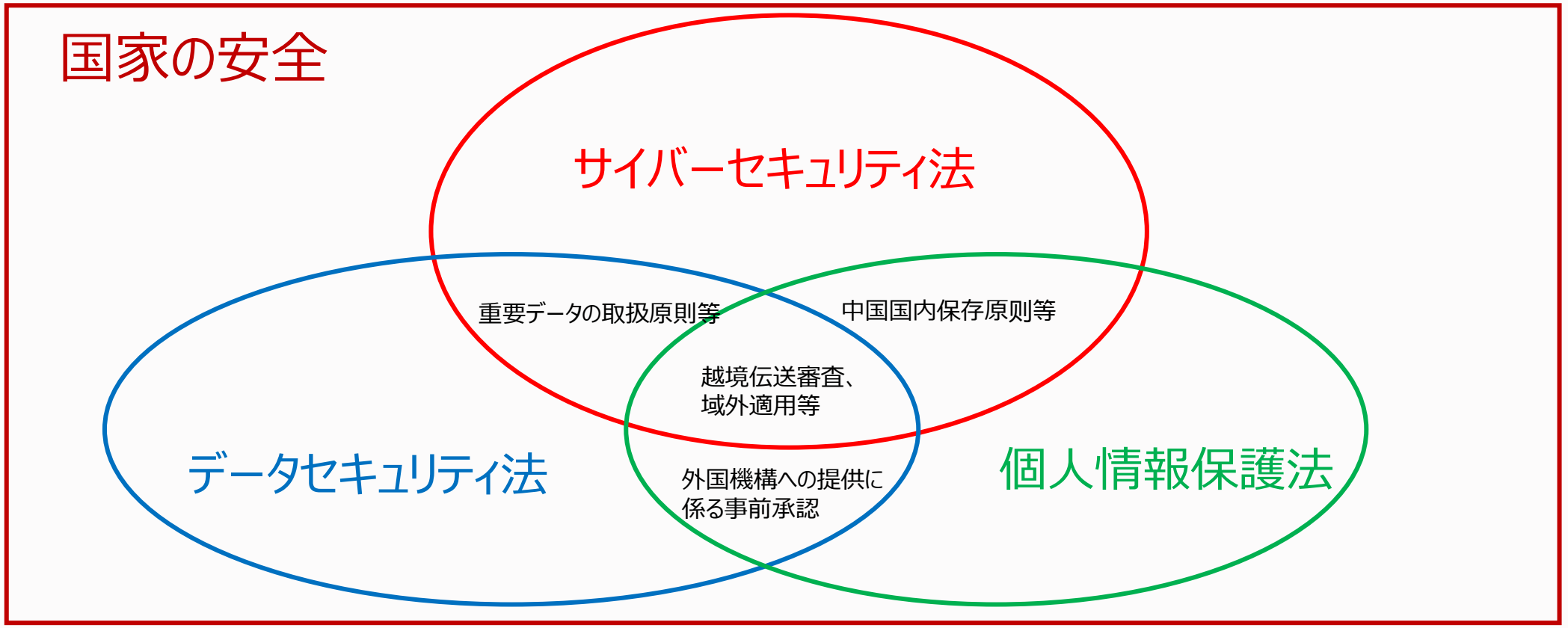
位置づけ：中国の情報規制の「三本の柱」

「サイバーセキュリティ法」（中華人民共和国主席令第53号 ）
- ◆ 2017年6月1日から施行
- ◆ 7章、計79条の規定により構成
- ◆ **「ネットワーク/システム」の運営の安全性、「ネットワーク情報」の内容の安全性を規定**

「データセキュリティ法」（中華人民共和国主席令第84号 ）
- ◆ 2021年9月1日から施行
- ◆ 7章、計55条の規定により構成
- ◆ **「データ」と「データの法的関係」を規定**

「個人情報保護法」（中華人民共和国主席令第91号 ）
- ◆ 2021年11月1日から施行
- ◆ 8章、計74条の規定により構成
- ◆ **「個人情報」の安全性を規定**

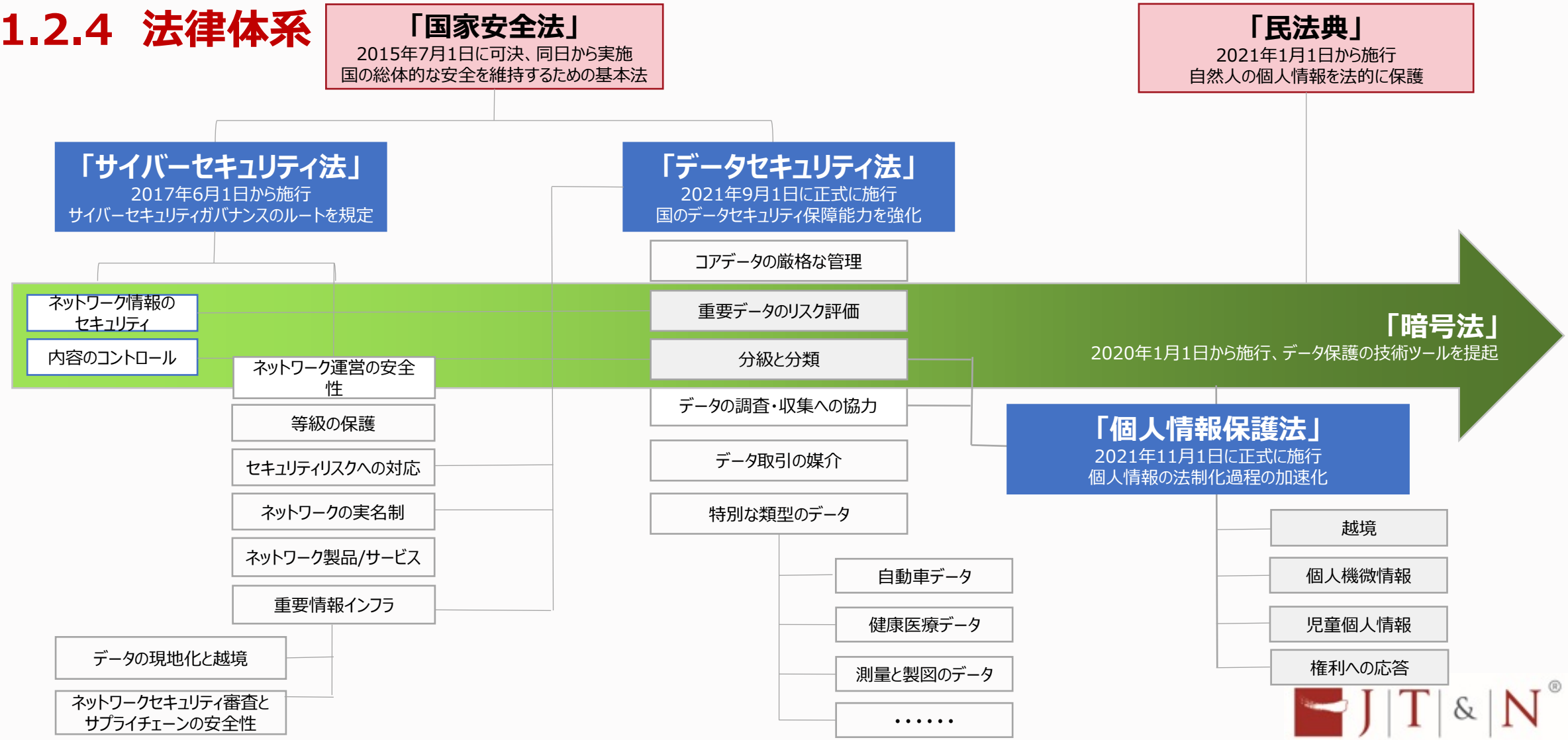
1.2.2 三法の関係図


国家の安全
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
重要データの取扱原則等
中国国内保存原則等
越境伝送審査、
域外適用等
外国機構への提供に
係る事前承認

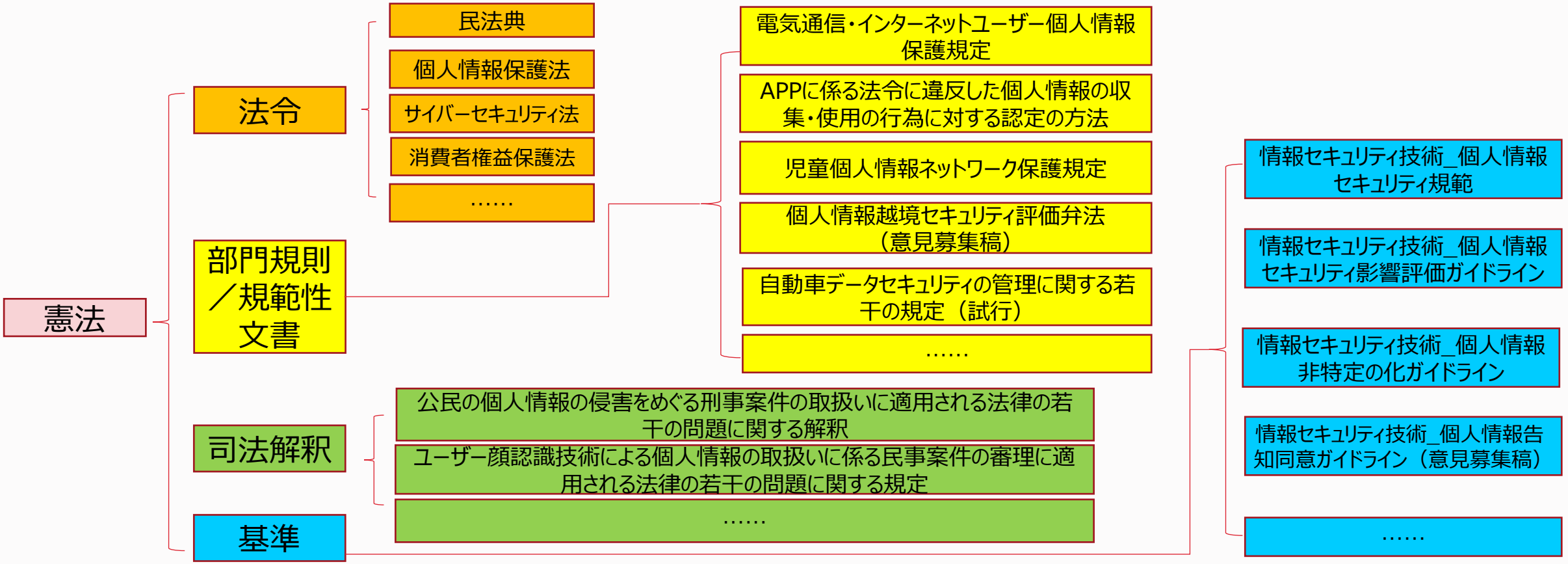
1.2.3 三法の適用範囲の比較

法律の名称	域内適用	域外適用
サイバーセキュリティ法	中国国内におけるネットワークの構築・運営・維持・使用およびサイバーセキュリティの監督・管理は、本法の適用を受ける。（第2条）	規定なし
データセキュリティ法	中国国内で行われるデータの取扱活動およびその安全に対する監督・管理は、本法の適用を受ける。（第2条1項）	中国国外で行われるデータ取扱活動が、中国の国家の安全・公共の利益または公民・組織の合法的な権益を侵害したときは、法的責任を法により追及する。（第2条2項）
個人情報保護法	中国国内における自然人の個人情報取扱活動は、本法の適用を受ける。（第3条1項）	中国国外における中国国内の自然人の個人情報の取扱活動も、次の各号に掲げる状況の一があったときは、本法の適用を受ける。（第3条2項） （一）中国国内の自然人への商品・役務の提供を目的としているとき。 （二）中国国内の自然人の行為を分析または評価しているとき。 （三）法律または行政法規の定めるその他の状況。

1.2.4 法律体系



1.2.5 個人情報保護の法律体系



1.2.6 三法にかかわる主管部門

◆ すなわち、国家インターネット情報弁公室。サイバーセキュリティ業務および関連の監督管理業務、個人情報保障業務の統一的な計画・調整を担当する。

◆ 自らの地区、自らの地域の業務範囲内におけるネットワークのデータセキュリティを担当する。

◆ 中央国家安全指導機構は、国のデータセキュリティ業務に関する意思決定・統括・議事の調整、国家のデータセキュリティ戦略と重大な方針・政策の研究・制定、その実施に対する指導、国家データセキュリティの重大な事項と業務の統括・調整、および国家のデータセキュリティ業務調整メカニズムの構築を行う。

◆ 具体的な業務の監督管理、
◆ 法執行の管理などを担当する。

◆ 自らの業界、自らの分野におけるネットワークのデータセキュリティを担当する。

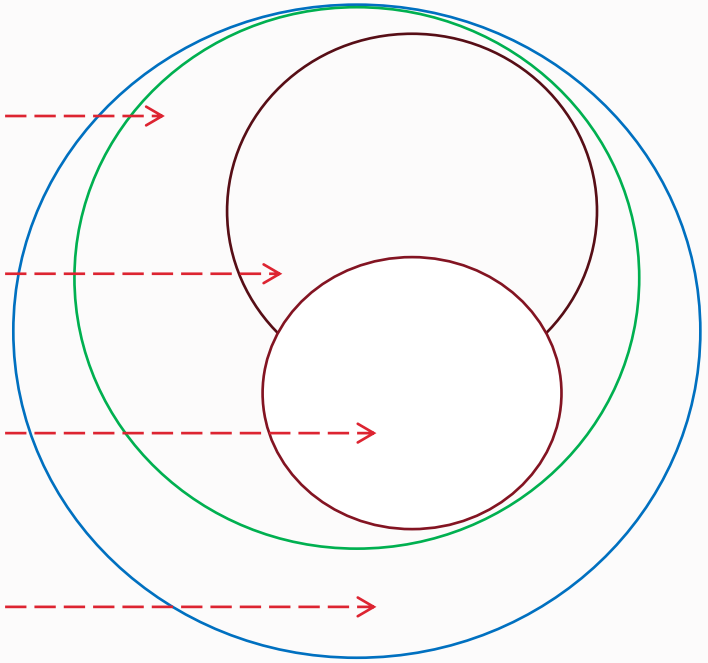
二、各法における重要な定義

2.1.1 ネットワークとは

- 法律上の「ネットワーク」とは、コンピュータその他の**情報端末および関連設備により構成**され、一定の規則およびプログラムに基づき情報の収集、保存、転送、交換、処理を行う**システム**をいう（「サイバーセキュリティ法」第76条）。
- ネットワークは、インターネットとは異なっている。実際のところ、インターネットはネットワークの一種にすぎない。ネットワークには、インターネットのほかにも、モバイル通信ネットワーク、インダストリアルインターネット、LAN などが含まれている。

2.1.2 ネットワーク運営者とは

- ◆ ネットワーク運営者
- ◆ 重要情報インフラ運営者
- ◆ ネットワーク製品やサービスの提供者
- ◆ 他の組織と個人

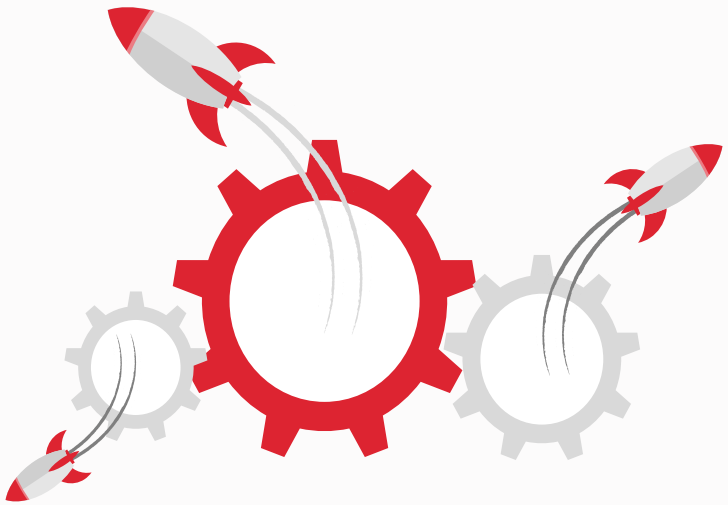


「ネットワーク運営者」とは、ネットワークの所有者、管理者およびネットワークサービスプロバイダをいう（「サイバーセキュリティ法」第76条）。

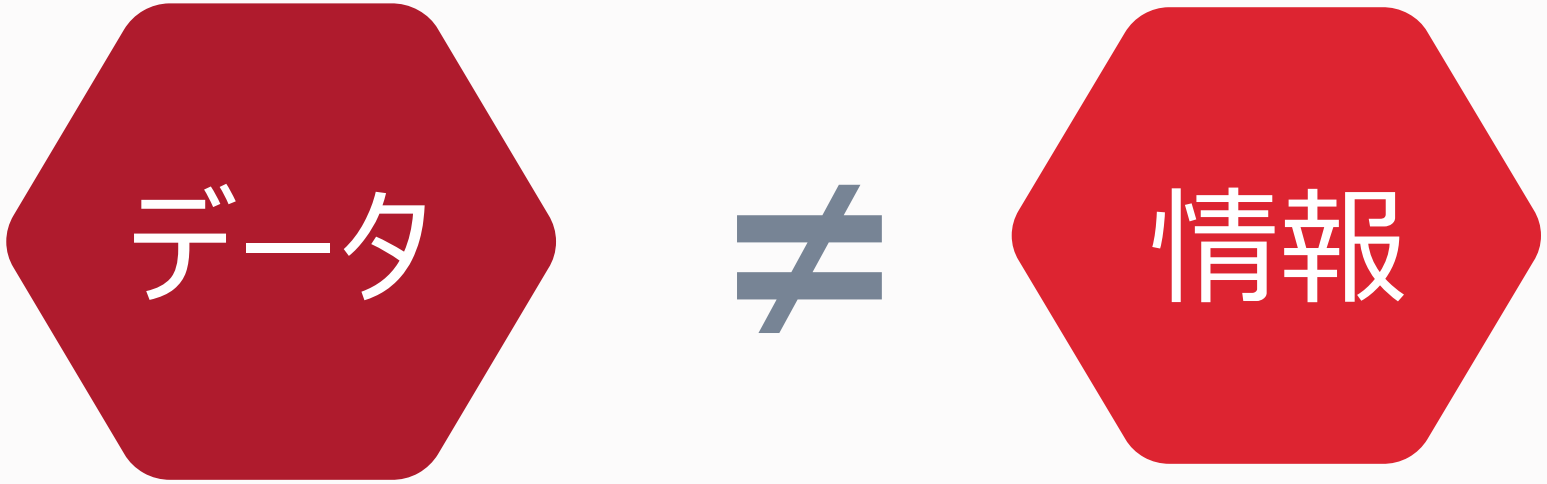
2.1.3 重要情報インフラ運営者とは

◆ 重要情報インフラとは、**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、電子行政、国防科学技術工業などの重要な業界および分野**に属しており、またはひとたび**破壊、機能喪失もしくはデータの漏えいに遭遇**した際に、**国の安全、 国の経済と人民の生活、もしくは公共の利益を著しく脅かす**おそれのあるその他の重要ネットワーク施設、情報システム等をいう。（「重要情報インフラ安全保障条例」第2条）。

◆ 重要情報インフラ運営者（Critical Information Infrastructure Operators。以下「**CIIO**」という。）とは、上記の重要情報インフラを運営する主体をいう。

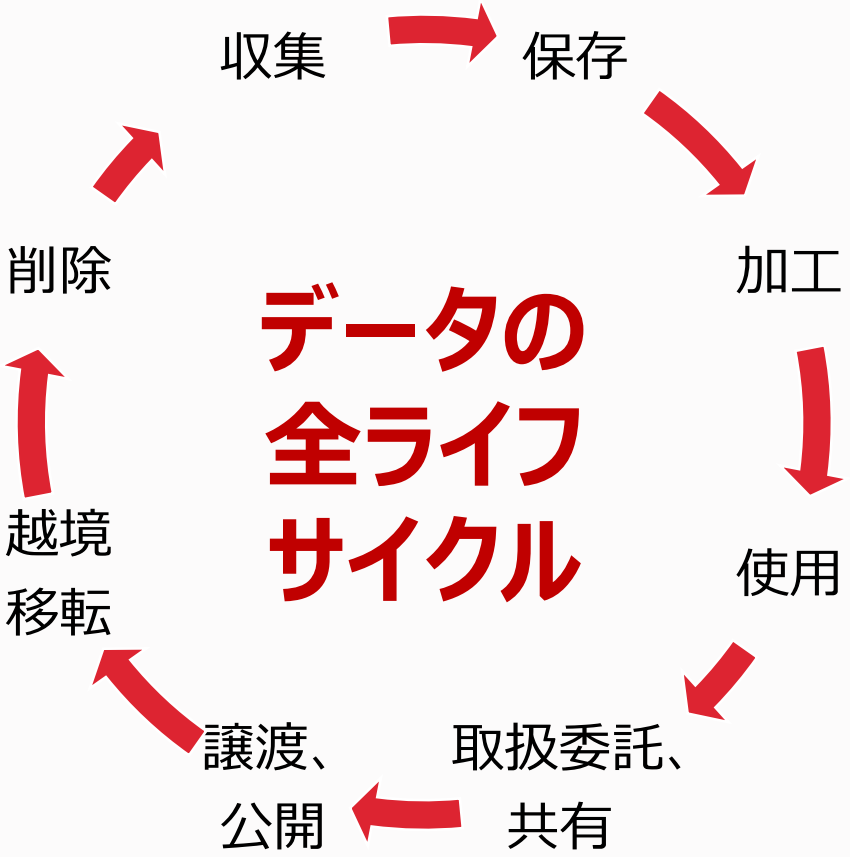


2.2.1.1 データとは



- 法律上のデータとは、電子その他の形式による**情報に対する記録**をいう （「データセキュリティ法」第3条）。
- 厳密には、情報の範囲は、データの範囲よりも広く、データは情報の媒体である。データは単に情報の一種の形式にすぎず、情報は他の形式をもって表現されることもある。

2.2.1.2 データのライフサイクルの全体像



2.2.1.3 社会的な倫理と公徳に対する尊重の重要性

「データセキュリティ法」第8条

データを取り扱うときは、法令の遵守、**社会的な公徳および倫理の尊重、商業道徳および職業道徳の遵守**、信義則の遵守、データセキュリティ保障義務の履行、ならびに社会的な責任の負担を行わなければならず、国家の安全、公共の利益または個人もしくは組織の合法的な権益を侵害してはならない。

「データセキュリティ法」第28条

データの取扱活動とデータの新技術の研究・開発は、経済社会の発展の促進に有利となり、人民の福祉水準を高め、**社会の公徳および倫理に適合していなければならない。**

2.2.2 重要データとは

「サイバーセキュリティ法」、「データセキュリティ法」においては、重要データの範囲が明確に定義されていないため、**国、各地方、および各業界による当該範囲にかかわるリストの策定が見込まれている**。

2021年8月20日に、国家インターネット情報弁公室は「自動車データセキュリティの管理に関する若干の規定（試行）」が公布された。同法は2021年10月1日から施行される。当該規定の第3条では、重要データが定義されており、自動車業界における重要データの定義が明確に規定されている。

重要データとは、ひとたび**改ざん・破壊・漏えい**され、または**違法に取得もしくは利用**されると、**国家の安全、公共利益または個人・組織の合法的な権益を侵害し得るデータ**をいう（「自動車データセキュリティの管理に関する若干の規定（試行）」第3条）。

2.2 「データセキュリティ法」

P23

2.2.3 重要データのイメージ

（「自動車データセキュリティの管理に関する若干の規定（試行）」および「情報安全技術_データ越境伝送セキュリティ評価ガイダンス（意見募集稿）」から抜粋）

業界	重要データの例	業界	重要データの例
自動車	• 軍事管理区、国防科学技術工業組織等の国家機密にかかわる組織、県級以上の共産党機関・政府行政機関などの**重要かつ機微な区域における地理情報**および**人・車両の流れ**のデータ • 交通量や物流などの**経済の運営状況を反映**しているデータ • 自動車の**充電ネットワークの運営データ** • 人相、ナンバープレートなどの**車外の映像・画像のデータ** • **10万人以上の個人情報** • 国務院の関係機関が指定している国家の安全、公共の利益または個人・組織の合法的な権益を侵害し得るその他のデータ	工業	• 世界的に先進的な水準にあり、国民の経済に重要な影響をもたらす工業の研究開発関連のプロジェクトまたはプランのデータ • 国際的な水準にあり、かつ、重大な経済的効果を生み出す科学研究成果の中核となる部分のデータ • 工業と科学技術の発展に向けた重点任務におけるセキュリティ関連の重要な科学技術にかかわるデータ
電子商取引	• 電子商取引プラットフォームにおける個人の登録情報（氏名、性別、年齢、住所、婚姻、学歴、職業、収入、口座、連絡先など） • 電子商取引記録、個人の消費習慣・嗜好、企業の経営などにかかわるデータ • 電子商取引における各当事者の信用記録、信用評価情報		

2.3.1.1 個人情報とは

- 個人情報とは、電子または他の方法をもって記録された**既に認識されており、または認識され得る自然人に係る各種の情報**をいう。ただし、匿名化処理後の情報は、この限りでない。（「個人情報保護法」第4条）。
- 個人プライバシーは主に、私的な情報または活動であり、その内容は個人が公開を望んでおらず、公共の利益にかかわらない。個人プライバシーは、情報のみに限定されず、個人の活動や私生活などの形式をもってしても、形成される。一方、個人情報の形式は、固定的である。

2.3.1.2 ：中国国内法上、最も厳密な個人情報の定義

関連規定	「個人情報保護法」	「民法典」	「サイバーセキュリティ法」
定義	第4条 個人情報とは、電子その他の方法をもって記録された既に認識されており、または認識され得る自然人に係る各種の情報をいう。	第一千零三十四条 個人情報とは、電子またはその他の方法をもって記録され、単独でまたはその他の情報と組み合わせて特定の自然人を認識することのできる各種の情報をいう 。	第76条 電子その他の方法をもって記録され、単独で、またはその他の情報と組み合わせて自然人（個人）の身分を認識することのできる各種の情報をいう。
コメント	これには認識可能な情報、および既に認識されている自然人にかかわる各種の情報が含まれている。範囲は最も広い。	認識可能な情報に限定されており、範囲は「個人情報保護法」に比べて狭い。	個人の身分を認識させる情報に限定されており、範囲は最も狭い。

2.3.1.2 ：中国国内法上、最も厳密な個人情報の定義

関連規定	「個人情報セキュリティ規範」	「公民の個人情報の侵害をめぐる刑事案件の取扱いに適用される法律の若干の問題に関する解釈」
定義	3.1 電子その他の方法により記録され、単独で、またはその他の情報と組み合わせて特定の自然人の身分を認識し、または特定の自然人の活動状況を反映することのできる各種の情報	第一条 「公民の個人情報」とは、電子またはその他の方法をもって記録され、単独で、またはその他の情報と組み合わせて特定の自然人の身分を認識し、または特定の自然人の活動状況を反映することのできる各種の情報をいう。
コメント	個人の身分を認識させる情報、および既に認識されている自然人の活動を反映している情報に限定されており、範囲は「個人情報保護法」に比べて狭い。	「個人情報セキュリティ規範」の定義と基本的には同様であり、範囲は「個人情報保護法」に比べて狭い。

2.3.1.3 個人情報の認定方法

認定方法：認識 + 関連性

「個人情報保護法」第4条の「個人情報」に関する定義によると、企業は「認識+関連性」の基準を使用し、これにより取り扱うデータの個人情報構成の成否を認定することができる：

① 認識の基準：**情報から個人が認識**される場合。すなわち、情報自体の特別性から、特定の自然人を認識することができるものである。たとえば、身分証明書番号などである。

② 関連性の基準：**個人から情報が生ずる**場合。すなわち、特定の自然人が既に知られており、当該特定の自然人が、自らの活動において生ずる情報である。たとえば、既に知られている特定の自然人の位置情報、通話記録などである。

【結論】

上述の二種類の状況のいずれかに該当する情報は、いずれも個人情報と判定されなければならない。

2.3.2.1 個人機微情報とは

「個人情報保護法」第28条

個人機微情報とは、ひとたび**漏えいし、または違法に使用**されたときは、自然人の**人格上の尊厳に対する侵害、または人身もしくは財産の安全性に対する脅威を容易に引き起こす**個人情報（生体認証、宗教・信仰、特定の身分、医療・健康、金融口座、行動履歴などの情報、および**十四歳未満の未成年者の個人情報**を含む。）をいう。

2.3 「個人情報保護法」

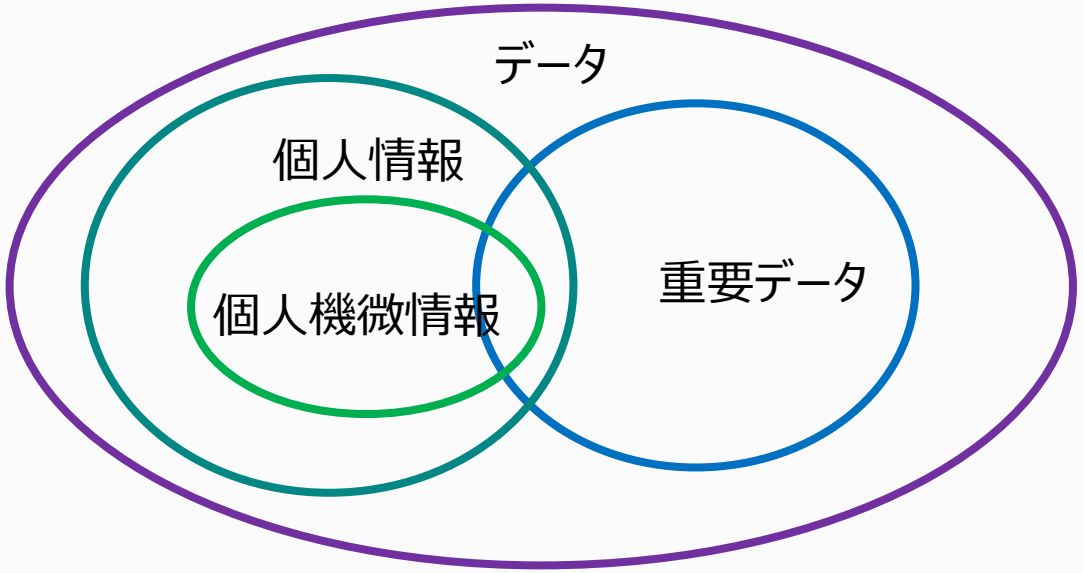
P29

2.3.2.2 個人情報および個人機微情報の例

赤字：個人機微情報

基本情報	氏名、誕生日、性別、民族、国籍、家族、住所、**電話番号**、メールアドレスなど
身分情報	**身分証明書、パスポート、労働許可証、社会保険カード、居住証**など
生物識別情報	**DNA、指紋、虹彩、顔識別特徴**など
ネットワーク身分識別情報	**システムアカウント、IPアドレス、電子メールアドレス、関連パスワード**など
健康生理情報	**疾病により生ずる関連記録、例えば病症、検査報告書、生育情報、過去の疾患、感染症の病歴**など
教育就職情報	個人の職業、職位、就職先、学歴、教育実務経験など
財産情報	**銀行口座、識別情報、預金情報、不動産情報、信用調査情報**など
通信情報	**通信記録および内容、**SMS、電子メールなど
連絡先情報	連絡先リスト、友達リスト、電子メールリストなど
ネットワーク利用情報	**ウェブサイトの閲覧記録**など
常用設備情報	ハードウェアのシリアルナンバー、デバイスのMACアドレスなど
位置情報	**行動履歴、高精度の位置情報、宿泊情報、緯度・経度**など
その他	**婚姻歴、宗教信仰、性的指向、未公開の犯罪記録**など

2.4 データと個人情報の関係性



① データと個人情報の関係性から見てみると、データには、個人情報が含まれている。

② 重要データと個人情報の関係性から見てみると、**一定の数量の個人情報は、重要データを構成する**可能性がある。たとえば、「自動車データセキュリティの管理に関する若干の規定（試行）」の第3条においては、**10万人以上の個人情報**が、重要データに属するという旨が規定されている。

三、各法における重要な制度

3.1.1 サイバーセキュリティ等級の意味

ネットワーク運営者は、破壊を受けた場合の個人・社会・国に対する影響の程度に応じて、サイバーセキュリティ保障能力の保有を保証する。

「サイバーセキュリティ法」

「サイバーセキュリティ等級保護実施条例」（意見募集稿）

「サイバーセキュリティ等級保護グレーディングガイドライン」

などの国家基準

情報システムの安全等級

↓

サイバーセキュリティ等級

ロ 情報システムの安全等級

- 新しい技術環境への適応の不能化
- モバイルアプリ、ビッグデータ、IoT、AI、ブロックチェーンなど

ロ サイバーセキュリティ等級

- 適用範囲の更なる拡大
- 基本的に前者の5段階の保護等級を踏襲

3.1.2 サイバーセキュリティ等級保護2.0

2019年12月1日をもって、以下の国家基準が正式に施行された。**「等級保護2.0」**制度の発効により、サイバーセキュリティ等級の評価には、新たな評価基準システムが適用されている。

「情報安全技術 サイバーセキュリティ等級保護基本要求」（ GB/T 22239-2019 ）
「情報安全技術 サイバーセキュリティ等級保護測定評価要求」（ GB/T 28448-2019 ）
「情報安全技術 サイバーセキュリティ等級保護実施ガイドライン」（ GB/T 25058-2019 ）
「情報安全技術 サイバーセキュリティ等級保護グレーディングガイドライン」（ GB/T 22240-2020 ）

「等級保護2.0」においては、**「等級保護1.0」**の5段階のセキュリティ等級に分かれた評価基準が、そのまま維持されており、セキュリティ一般要求、ならびにクラウドコンピューティング、モバイルネットワーク、IoT、ビッグデータ、および産業用制御システムに対する標準的な評価システムが形成されている。

いまだに等級保護を届け出ておらず、または等級保護評価の実施後に、再評価を毎年行わなければならない情報システムの運営者は、これへの留意が必要である。

3.1.3 サイバーセキュリティ等級保護における基本的な義務

一般的な安全保障義務

サイバーセキュリティ責任者の指定、サイバーセキュリティ等級保障業務責任制の確立、
サイバーセキュリティの責任追及制度の実施など

自主検査

サイバーセキュリティ等級保護制度の状況と、サイバーセキュリティの状況に対する
少なくとも一年に一回の自主検査の実施、および届出機関への報告の義務

データと情報のセキュリティ保障

重要データと個人情報のセキュリティ保障制度、保障措置、オフサイトでのバックアップなど

新たな技術とその応用を通じたセキュリティリスクの管理・制御

措置の採択、新たな技術とその応用（たとえば、クラウドコンピューティング、ビッグデータ、AI、IoTなど）を通じたセキュリティリスクの管理・制御、および安全上の潜在的なリスクの解消の義務

3.1.4 サイバーセキュリティ等級保護－3級以上の追加義務

1.特別安全保障義務

ネットワーク安全管理の責任者と重要ポストの人員に対する安全背景審査の実施、特定のポストに対する資格取得義務制度等の実施

2.評価結果の届出

毎年一回のサイバーセキュリティ等級評価の実施、業務状況と評価結果の届出機関への報告

3.製品とサービスの調達・使用上の安全要求

セキュリティ保障等級に応じたネットワーク関連の製品・サービスの採用、重要な製品に対する測定評価等の実施

4.技術メンテナンス

中国国内における技術メンテナンスの実施、中国国外からの遠隔サポートの不能性、必要時におけるネットワークセキュリティ評価の実施

5.検査・事前警報、情報通報

関連制度の確立、公安機関と業界主管部門への関連情報の報告、サイバーセキュリティインシデントの報告

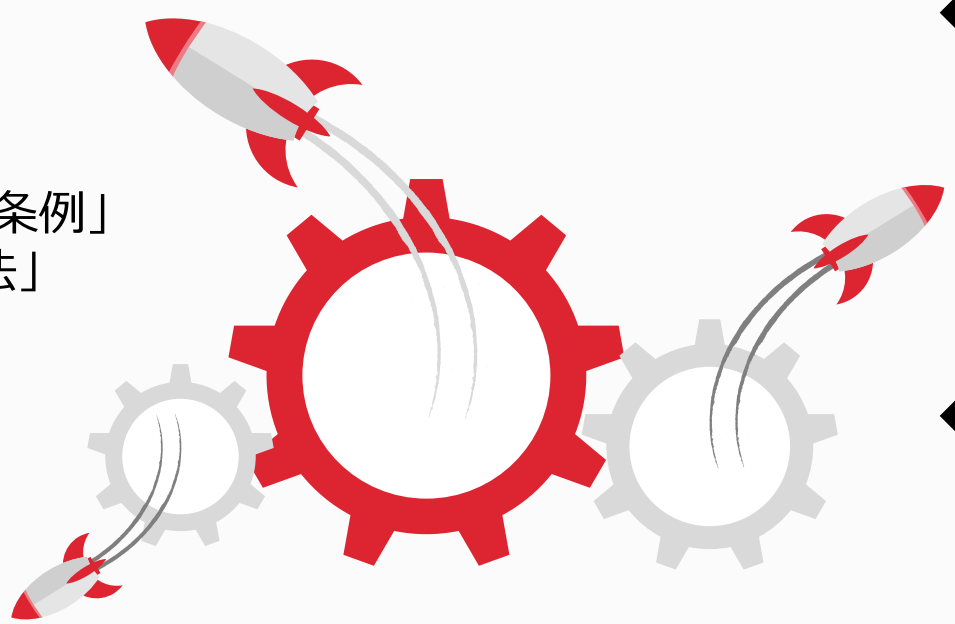
6.緊急対応

サイバーセキュリティ緊急対応プランの制定、サイバーセキュリティ緊急対応演習の定期的な実施

3.2.1 重要情報インフラの認定規則

法的根拠

◆「サイバーセキュリティ法」
◆「重要情報インフラ安全保護条例」
◆「サイバーセキュリティ審査弁法」



現状

◆「重要情報インフラ安全保護条例」は、2021年8月17日に正式に公布され、2021年9月1日に施行される予定である。ただし、当該条例において、**重要情報インフラ（CII）の認定規則がまだ確定されていない**。
◆これから、重要業界および分野の主管部門、管理監督部門が公布する重要情報インフラの認定規則を注意する必要がある。

3.2.2 CIIOの義務

個人情報および重要データ関連

- ◆ 個人情報および重要データの中国国内における保存
- ◆ 越境伝送時のセキュリティ評価

特別安全保障制度

- ◆ 専門の安全管理機構の設立、責任者の配置
- ◆ 従業員に対する定期的なサイバーセキュリティ教育、技術研修、考査
- ◆ 重要なシステムとデータベースに対する災害対策のためのバックアップの作成
- ◆ サイバーセキュリティインシデントへの緊急対応プランの制定、定期的な演習の実施

セキュリティ評価

- ◆ サイバーセキュリティとその関連リスクに対する年に一回以上の測定評価

3.3 サイバーセキュリティ審査制度

P38

現行の規定（2020/6/1）

「サイバーセキュリティ審査弁法」第2条

重要情報インフラの運営者が**ネットワーク関連の製品・サービスを調達する場合**において、**国家の安全に影響を及ぼす可能性があるとき**は、本法に従ってサイバーセキュリティ審査を行わなければならない。

第二次改定（意見募集稿）（2021/7/10）

第二次改定の意見募集稿の第2条、第6条

重要情報インフラの運営者がネットワーク関連の製品・サービスを調達し、**データの取扱者がデータを取り扱う場合において、**国家の安全に影響を及ぼす可能性があるときは、本法に従ってサイバーセキュリティ審査を行わなければならない。

100万人以上のユーザーの個人情報を保有する運営者は、中国国外に上場する場合、その旨をサイバーセキュリティ審査弁公室に報告し、サイバーセキュリティ審査を受けなければならない。

3.4 データ分類・分級保護制度

P39

国家核心データ

重要データ

その他データ

「サイバーセキュリティ法」第21条

国は、サイバーセキュリティ等級保護制度を実施する。ネットワーク運営者はサイバーセキュリティ等級保護制度の規定に応じ、以下の安全保障義務を履行し、ネットワークが妨害、破壊または無許可アクセスを受けたことを避止し、**ネットワークデータの漏えいまたは窃取、改ざんを防止**する：…（四）**データ分類、重要データバックアップ**及暗号化等の措置の実施

「データセキュリティ法」第21条

国は、データ分類分級保護制度を構築し、データの経済社会発展における重要さ、及びひとたび改ざん・破壊・漏洩・違法取得・違法利用されたときの危険性に基づき、**データ分類分級保護を実行**する。

国家安全、国民経済の命脈、重要な民生、重大な公共利益等のデータは国家核心データであり、さらに厳格な管理制度を実行する。

3.5 データセキュリティ審査制度

P40

データセキュリティ審査制度

「データセキュリティ法」第24条

国はデータセキュリティ審査制度を構築し、国家安全に影響を及ぼし、又は及ぼしうるデータ取扱活動について国家安全審査を実施する。

◆「サイバーセキュリティ審査方法」（現行）：**重要情報インフラ運営者**の調達するサイバーセキュリティ製品およびサービスを対象とする安全審査制度

3.6 重要データ取扱活動リスク評価および報告制度

「データセキュリティ法」第30条

重要データ取扱者は、関連規定に基づき、そのデータ取扱活動について**定期的にリスク評価**を行い、関連主管部門**にリスク評価報告書を提出**しなければならない。

評価報告書には、以下の内容を含めなければならない。

（一）取り扱う重要データの種類・数量

（二）データ取扱活動の状況

（三）直面するデータセキュリティリスク

（四）その対応措置等

「自動車データセキュリティ管理若干規定」第10条、第13条

自動車データ取扱者は重要データ取扱活動を行うとき、規定に従ってリスク評価を行い、かつ省、自治区、直轄市のインターネット情報部門と関連部門に対してリスク評価報告を提出しなければならない。

自動車データ取扱者は重要データの取扱活動を行うにあたって、**毎年12月15日までに**、当年度の自動車データセキュリティ管理に関する次の状況を省、自治区、直轄市のインターネット情報部門と関連部門に**報告**しなければならない。

3.7 国外の個人情報取扱者の中国における機構設立および届出の制度

P42

「個人情報保護法」第3条第2項

中国国外における中国国内の自然人の個人情報の取扱活動も、次の各号に掲げる状況の一があったときは、本法の適用を受ける。

（一）中国国内の自然人への商品・役務の提供を目的としているとき。

（二）中国国内の自然人の行為を分析又は評価しているとき。

（三）法律又は行政法規の定めるその他の状況

「個人情報保護法」第53条

本法第三条第二項の定める中国国外の個人情報の取扱者は、①**中国国内に専門機構又は指定代表者を設け**、個人情報保護関連事務の取扱いを担当させ、**関連機構の名称、代表者の氏名、連絡方法などを**個人情報保護職責履行部門に**届け出**なければならない。

3.8 個人情報保護影響評価制度

P43

「個人情報保護法」第55条

次の各号に掲げる状況の一に該当するときは、個人情報の取扱者は、**個人情報保護影響評価を事前に行い**、自らの取扱状況に対し、記録を行わなければならない。

（一）**個人機微情報**の取扱い

（二）個人情報を利用した**自動化された意思決定の実施**

（三）個人情報取扱いの**委託、その他の個人情報取扱者への**個人情報の**提供**、**個人情報の公開**

（四）**中国国外への個人情報**の提供

（五）個人の権益に重大な影響を及ぼすその他の個人情報取扱活動

「個人情報保護法」第56条

個人情報保護影響評価には、次の各号に掲げる内容が含まれていなければならない。

（一）個人情報取扱いの目的・方法等の合法性・正当性・必要性の有無

（二）個人権益に対　する影響及びセキュリティリスク

（三）採択した保護措置の合法性・有効性、リスクの程度への相応性

個人情報保護影響評価報告書と取扱状況記録は、**少なくとも三年保存**しなければならない。

3.9 重要なインターネットプラットフォームサービス提供者への特別管理制度

P44

義務①

主に外部の者から構成される独立的な機構の設立、同機構による個人情報取扱行為の監視

義務②

法律または行政法規に著しく違反して個人情報を取り扱ったプラットフォーム上の商品・役務の提供者に対するサービス提供の停止

義務③

個人情報の保護にかかわる社会的責任報告書の定期的な公開、社会からの監視の受入れ

◆ **適用対象：基礎的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、ユーザー数が膨大で、かつ、業務の内容が複雑な個人情報の取扱者**

3.10 一部の重要制度に対する比較

P45

3.10.1 比較の一

	サイバーセキュリティ審査	データセキュリティ審査	重要データ取扱活動リスク評価	個人情報保護影響評価
設定の目的	国家の安全に影響を及ぼし、または及ぼし得るリスクの軽減	国家の安全に影響を及ぼし、または及ぼし得るデータ取扱活動のリスクの軽減	重要データ取扱者が直面するデータセキュリティリスクの明確化	個人の権益に重大な影響を及ぼし、または及ぼし得る個人情報取扱活動のリスクの明確化
制度の内容	CIIOは、ネットワーク製品またはサービスを調達し、国家の安全に影響を及ぼす可能性があるときは、サイバーセキュリティ審査を通過しなければならない。	国は、データセキュリティ審査制度を構築し、国家の安全に影響を及ぼし、または及ぼし得るデータ取扱活動に対し、国家安全審査を実施する。	重要データ取扱者は、関連規定に基づき、自らのデータ取扱活動に対する定期的なリスク評価を行い、リスク評価報告書を主管部門に提出しなければならない。	個人情報の取扱者は、個人情報保護影響評価を事前に行い、自らの取扱状況に対し、記録を行わなければならない。
根拠	◆「サイバーセキュリティ法」第35条 ◆「サイバーセキュリティ審査弁法」およびその修正案の意見募集稿	「データセキュリティ法」第24条	◆「データセキュリティ法」第30条 ◆「自動車データセキュリティの管理に関する若干の規定」第10条、第13条	「個人情報保護法」第55条、第56条

3.10 一部の重要制度に対する比較

P46

3.10.2 比較の二

	サイバーセキュリティ審査	データセキュリティ審査	重要データ取扱活動リスク評価	個人情報保護影響評価
義務の主体	◆ CIIO ◆ 中国国外における上場を予定している100万人分のユーザーの個人情報を所有する運営者 ◆ データの取扱者	データの取扱者	重要データの取扱者	個人情報の取扱者
審査・評価が必要な状況	◆ ネットワーク製品またはサービスを調達し、国家の安全に影響を及ぼす可能性があるとき ◆ データ取扱者がデータ取扱活動を展開し、国家の安全に影響を及ぼす可能性があるとき ◆ 100万人分のユーザーの個人情報を所有しており、かつ、中国国外における上場を予定している運営者	データの取扱活動を展開し、国家の安全に影響を及ぼし、または及ぼし得るとき	重要データ取扱活動に対する定期的なリスク評価を行うとき	◆ 個人機微情報の取扱時 ◆ 個人情報を利用した自動化された意思決定の実施時 ◆ 個人情報取扱いの委託時 その他の個人情報取扱者への個人情報の提供時 個人情報の公開時 ◆ 中国国外への個人情報の提供時 ◆ 個人の権益に重大な影響を及ぼすその他の個人情報の取扱時

3.10 一部の重要制度に対する比較

P47

3.10.3 比較の三

	サイバーセキュリティ審査	データセキュリティ審査	重要データ取扱活動リスク評価	個人情報保護影響評価
審査・評価内容	◆ 製品・サービスの利用後に、重要情報インフラに対してもたらす可能性のあるリスクと危険性 ◆ 中国国外での上場後に、重要情報インフラ、核心データ、重要データまたは大量の個人情報が中国国外の政府によって制御されるリスク	核心データ、重要データまたは大量の個人情報が、窃取・漏えい・破損され、または違法に利用され、もしくは中国国外に持ち出されるリスク	◆ 取り扱う重要データの種類・数量 ◆ データ取扱活動の状況 ◆ 直面するデータセキュリティリスクおよびその対応措置など	◆ 個人情報取扱いの目的・方法等の合法性・正当性・必要性の有無 ◆ 個人権益に対する影響およびセキュリティリスク ◆ 採択した保護措置の合法性・有効性、リスクの程度との相応性
届出要求	関連資料のサイバーセキュリティ審査弁公室への申告	明確な規定なし	◆ 関連主管部門にリスク評価報告書を提出しなければならない。 ◆ 自動車データの取扱者は、重要データを取り扱ったときは、**毎年の12月15日までに**、省・自治区・直轄市のインターネット情報部門と関連部門に報告しなければならない。	明確な規定なし。ただし、個人情報保護影響評価報告書と取扱状況記録は、少なくとも三年間保存しなければならない。

3.11 各法の間における責任者に対する定義の比較

P48

法律	適用範囲		
	役職名	法的規定	職責
サイバーセキュリティ法	サイバーセキュリティ責任者	第21条1項 ネットワーク運営者は、サイバーセキュリティの等級ごとの保障制度の要求に応じ、次の各号に掲げる安全保障義務を履行する。 （一）内部安全管理制度と実務規程の制定、**サイバーセキュリティ責任者**の確定	ネットワークセキュリティの保障
データセキュリティ法	データセキュリティ責任者	第27条2項 重要データ取扱者は、**データセキュリティ責任者**と管理機構を明確にし、データセキュリティ保障責任の履行を徹底化しなければならない。	データセキュリティの保障
個人情報保護法	個人情報責任者	第52条 個人情報の取扱数が国家インターネット情報部門の定める数量に達した個人情報の取扱者は、**個人情報保護責任者**を指定し……	個人情報セキュリティの保障

【コメント】 ① 各法間の関係、および個人情報と重要データの関係性を踏まえて見てみると、上記の責任者の職責には、重複した箇所がある。

② 法律上、上記の責任者の兼任は禁止されておらず、兼任することができる。

3.12 各法の間における法的責任の比較

P49

事項		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
過料の上限	企業	100万元	1000万元	**5000万元以下、または前年度の売上高の5%以下のうちのいずれか高い額**
	責任者	10万元	100万元	100万元（第66条）
その他の事項		◆ 関連業務の一時停止 ◆ 営業停止・整理 ◆ ウェブサイトの閉鎖 ◆ 業務許可または営業許可証の取消命令	左記ものと同様	◆ 左記のものと同様 ◆ 一定期間中の関係会社における董事・監事・高級管理職員・個人情報保護責任者の担当の禁止 ◆ 信用記録への記載、同記録の公示

四、情報の収集・保存・利用の留意点

4.1.1 データ（重要データを含む）の収集

「サイバーセキュリティ法」および「データセキュリティ法」には、重要データの収集について、データ取扱者に特別な法定義務を定められていない。

「サイバーセキュリティ法」第27条

いかなる個人及び組織も、他人のネットワークへの不正侵入、他人のネットワークの正常な機能の妨害、**ネットワークデータの窃取**等、サイバーセキュリティを脅かす活動を**行ってはならない**。

「データセキュリティ法」第32条

如何なる組織・個人によるデータ収集も、**合法・正当な方法を採用**しなければならず、窃取又はその他違法な方法によりデータを取得してはならない。

法律・行政法規が、収集・使用されるデータの目的・範囲について規定を設けている場合、**法律・行政法規の規定する目的・範囲内でデータを収集**・使用しなければならない。

4.1.2 個人情報の収集

◆原則 ⇒ 同意を取得する

「個人情報保護法」第13条第1項第（1）号および第14条

◆例外 ⇒ 同意を取得する必要がない

「個人情報保護法」第13条第1項第（2）号～第（7）号

（二）個人を**一方の当事者とする契約の締結若しくは履行**に必要**不可欠**なとき、又は法により制定若しくは締結した**労働規則制度若しくは労働協約に従った人的資源管理の実施**に必要**不可欠**なとき。

（三）**法定の職責又は義務の履行**に必要**不可欠**なとき。

（四）**突発的な公衆衛生事件への対応**又は**緊急の状況下における自然人の生命・健康若しくは財産の安全性の保護**に必要不可欠なとき。

（五）**公益のために報道、世論の監督**などの行為を実施し、合理的な範囲において個人情報を取り扱うとき。

（六）本法の規定の下、**合理的な範囲において個人が自ら公開した個人情報、又は既に合法的に公開されているその他の個人情報**を取り扱うとき。

（七）法律又は行政法規の定めるその他の状況。

4.1.3 個人機微情報の収集

根拠：「個人情報保護法」第28条第2項

原則：ただ特定の目的及び十分な必要性が存在しており、かつ、厳格な保護措置が採択されている状況下においてのみ、個人情報の取扱者は、個人機微情報を初めて取り扱うことができる。

同意の条件：

単独同意または書面同意

「個人情報保護法」第29条

個人機微情報の取扱いは、個人の**単独の同意を取得**しなければならない。ただし、法律又は行政法規が、個人機微情報の取扱時における**書面の同意の取得義務を定めているときは、その規定に従う**。

告知の条件：

「個人情報保護法」第17条

＋以下の内容。

「個人情報保護法」第30条

個人機微情報の**取扱いの必要性**、及び**個人の権益に対する影響**を個人に告知しなければならない。ただし、**法律の規定に従って個人に告知しないことができるときは、この限りでない**。

未成年者への取扱：

「個人情報保護法」第31条

個人情報の取扱者は、**十四歳未満の未成年者の個人情報を取り扱う**ときは、未成年者の**父母又は他の後見人の同意を取得**しなければならない。

4.1.4 情報収集の比較

法律	対象	共通点	相違点
データセキュリティ法	データ、重要データ	合法的かつ正当な方法の採用、窃取またはその他違法な方法の不採用	◆ 収集時の同意の不要性 ◆ 収集範囲の不制限
個人情報保護法	個人情報	合法的かつ正当な方法の採用、窃取またはその他違法な方法の不採用	◆ 収集時の同意の必要性（例外あり） ◆ **最小の範囲への限定**、過度の収集の禁止
個人情報保護法	個人機微情報	合法的かつ正当な方法の採用、窃取またはその他違法な方法の不採用	◆ 特定の目的及び十分な必要性が存在しており、かつ、厳格な保護措置が採択されている状況下においてのみという初めて収集できる前提条件 ◆ **最小の範囲への限定**、過度の収集の禁止 ◆ 収集時の単独の同意または書面の同意の必要性 ◆ 告知内容の広さおよび厳しさ

4.2.1 データの保存

「サイバーセキュリティ法」第21条

ネットワーク運営者は、サイバーセキュリティ等級保護制度の要件に基づき、次の各号に掲げる安全保護義務を履行し、ネットワークが妨害、破壊又は無許可アクセスを受けないよう保障し、**ネットワークデータの漏えい又は窃取、改ざんを防止しなければならない**。

……

（四）**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。

……

「データセキュリティ法」第27条

データ取扱は、……**相応する技術措置**及び**その他の必要措置**を講じ、データセキュリティを保障しなければならない。インターネット等の情報ネットワークを利用してデータ取扱活動を行う場合、サイバーセキュリティ等級保護制度に基づいた上、上記データセキュリティ保護義務を履行しなければならない。

4.2.2 重要データの保存

根拠：「サイバーセキュリティ法」第37条、「データセキュリティ法」第31条

原則：中国での運営において収集および発生した重要データは、中国で保存する。

「サイバーセキュリティ法」第37条

重要情報インフラの運営者は、中華人民共和国**国内での運営において収集及び発生した**個人情報及び**重要データ**を、中華人民共和国**国内で保存**しなければならない。

「データセキュリティ法」第31条

重要情報インフラ施設運営者による、中国国内での運営の過程において収集・発生した**重要データの中国国外への移転に対する安全管理**については、**「サイバーセキュリティ法」の規定を適用**する。

「自動車データセキュリティ管理若干規定」第11条

重要データは、法により中国国内に保存しなければならない。業務上の需要により中国国外への提供が確かに必要である場合、国家インターネット情報部門と国務院の関連部門が共同で実施するセキュリティ評価を通過しなければならない。

4.2.3 個人情報の保存

根拠：「個人情報保護法」第19条、第40条、第47条および第51条

1	最短保存期間	◆ 最短期間で保存 ◆ 保存期限が満了してから、削除する
2	分 類 管 理	◆ 収集してから、個人情報に対する分類管理を実施する
3	技術措置の採択	◆ 個人機微情報を収集、転送する際に、暗号化、非識別化などのセキュリティ技術措置を講じる
4	中国国内で保存	◆ CIIO取り扱う個人情報の数量が国家インターネット情報部門の定める数量に達している個人情報の取扱者は、国内での運営において収集及び発生した個人情報を、中華人民共和国国内で保存しなければならない

4.2.4 個人機微情報の保存

「個人情報安全規範」（GB/T 35273-2020）第6.3条

- ◆ 個人機微情報を収集、転送する際に、暗号化等安全措置を講じなければならない。
- ◆ 個人生体認証情報は個人の身分情報と分けて保存しなければならない。
- ◆ 個人の生体認証情報を保存する場合、個人の生体情報の要約のみを保存するなど、技術的な手段を講じて処理した後に保存する必要がある。

4.2.5 情報保存の比較

法律	対象	共通点	相違点
サイバーセキュリティ法	データ、重要データ	◆ CIIOの重要データの中国国内における保存 ◆ データの分類管理 ◆ 技術的な措置の採択	◆ 保存期間の不強制 ◆ 業務停止時の削除の不強制
データセキュリティ法	データ、重要データ	◆ CIIOの重要データの中国国内における保存 ◆ データの分類管理 ◆ 技術的な措置の採択	◆ 保存期間の不強制 ◆ 業務停止時の削除の不強制
個人情報保護法	個人情報、個人機微情報	◆ CIIOおよび特別な個人情報取扱者の個人情報の中国国内における保存 ◆ 個人情報の分類管理 ◆ 技術的な措置の採択	◆ 保存期間の取扱目的の実現に要する期間への**最短化** ◆ 業務停止時の削除

4.3.1 データおよび重要データの利用

根拠：「データセキュリティ法」第28条、第32条第2項

原則：データおよび重要データの利用は、法令の規定を順守し、社会公徳および論理に適合しなければならない。

「データセキュリティ法」第28条

データ取扱活動及びデータ新技術の研究開発は、経済社会の発展の促進に有利であり、人民の**社会の公徳及び倫理に適合**しなければならない。

「データセキュリティ法」第32条第2項

法律・行政法規が、収集・使用されるデータの目的・範囲について規定を設けている場合、**法律・行政法規の規定する目的・範囲内でデータを**収集・**使用しなければならない**。

4.3.2.1 個人情報および個人機微情報の利用

アクセスコントロール

◆内部管理（必要最低限）、内部承認プロセス

◆個人機微情報は、業務の流れのニーズに応じてアクセス権限を付与する（例：ユーザーの苦情があったときに限り、個人機微情報にアクセス可能）

個人情報表示

◆技術的な措置の採択

使用制限

◆取決めた範囲を超えて個人情報を使用する場合には、個人から同意を再度取得しなければならない。

4.3.2.1 個人機微情報の利用に関連する判例

郭兵と杭州野生動物世界有限会社との間におけるサービス契約紛争

（〈 2019 〉浙0111民初6971号、〈2020〉浙01民終10940号）

【原告と被告】一審の原告（二審の上訴人）：郭兵

一審の被告（二審の上訴人）：杭州野生動物世界有限会社

【事例の概要】

2019年4月に、郭兵氏は杭州野生動物世界の二人用年間フリーパスカードを購入し、指紋の認識を通じた入園の方法を確定した。二人は氏名、身分証番号、電話番号などを記し、指紋を登録し、写真を撮影した。2019年の7月と10月に、杭州野生動物世界は、二度にわたって郭兵氏にメッセージを発送し、**年間フリーパスカード入園認識システムの変更事項を通知して顔認識システムの始動を要求し、これを行わなければ、正常に入園することができなくなる**という旨を告げた。**郭兵氏は顔の情報が機微性の高い個人プライバシーに属しているものと考え、顔認識の受入れに同意せず、カードの払戻しを動物園側に要求**した。双方の当事者の協議が成立しなかったことから、2019年10月28日に郭兵氏は、人民法院に訴訟を提起した。

4.3.2.1 個人機微情報の利用に関連する判例

【判決の結果】

一審において、人民法院は杭州野生動物世界有限会社による契約の利益損失および交通費である合計1038元の郭兵氏への賠償、および郭兵氏が指紋年間フリーパスカードの取扱時に提出した写真を含む顔の部分の特徴を表す情報の削除を判決した。

二審において、人民法院は一審における上述の判決の維持を基礎とし、原告が指紋年間フリーパスカードの取扱時に提出した指紋認識情報の削除を判決を通じて被告に命じた。（報道によると、郭兵氏は再審を申請している。）

【事例の啓示】

個人情報の取扱者として、企業は顔認識情報等の個人情報を慎重に取り扱い、「合法性・正当性・必要性」という三大原則を遵守しなければならない。顔認識技術を利用した個人情報の収集または取扱いが必要となった際には、主体的に注意を喚起し、その事情を当該個人に明かさなければならない。認識方法の増加等の目的によりサービス協議書を更新する際には、個人の選択権を保留し、非顔認識等のその他の身分認識方法を同時に提供し、これにより個人の選択への使用に供するよう注意しなければならない。このほかにも、企業は個人情報に対するセキュリティ保障を強化し、データの漏えいを厳格に防止しなければならない。

4.3.2.2 個人情報の共同取扱の場合

根拠：「個人情報保護法」第20条

共同取扱の**契約書**を締結し、各自の権利・義務を取り決める

＋

各個人情報取扱者が**連帯責任**を法により負担する

4.3.2.3 個人情報の委託取扱の場合

根拠：「個人情報保護法」第21条

委託取扱の**契約書**を締結し、各自の権利・義務を取り決める

＋

受託者は、取り決めた取扱いの**目的・方法などを超過して個人情報**を取り扱ってはならない。

4.3.2.4 個人情報の第三者へ提供する場合

根拠：「個人情報保護法」第23条

第三者の関連情報を個人に**告知** ＋ 単独の**同意**

◆「個人情報保護法」においては、単独の同意の定義は、明確に規定されていない。

◆単独の同意は、**「無差別的同意」または「一括同意」の逆**でなければならない。すなわち、相応の個人情報の取扱行為は、単独の同意の仕組みが備わっていなければならず、その他の個人情報の取扱行為と混合させて個人情報の主体の同意を取得することはできない。

4.3.2.5 個人情報を公開する場合

根拠：「個人情報保護法」第25条

原則として、
禁止

＋

例外として、
単独同意
の取得

4.3.2.6 個人情報の自動化の意思決定を行う場合

根拠：「個人情報保護法」第24条

意思決定の透明性、及び結果の公平性・公正性を保証

＋

非対象化の選択肢又は簡便な拒絶方法を提供

4.3.2.6 自動化された意思決定に関連する判例

【事例の概要】

原告である胡氏は、被告である上海携程商務有限公司（Ctrip）のVIP顧客であった（15%Offの優遇価格の享受が可能）。2020年7月に、原告はCtripのAPPを通じて舟山ヒルトンホテルの豪華湖景クイーンサイズルームをブッキングし、価格である2889元を支払った。しかしその後に、原告はホテルの実際の公示価格が、ただ1377.63元のみであったことに気が付いた。被告に苦情をしたところ、被告は「自社がプラットフォーム業者であり、本件ブッキング契約の相手方ではない」などという旨を理由とし、ただ一部の差額のみを返還した。胡氏は、被告が必要ではない胡氏の個人情報を収集し、ビッグデータを通じた「常連客への差別行為」（中国語：殺熟）を行ったことなどを理由とし、同社を相手取って人民法院に提訴した。

4.3.2.6 自動化された意思決定に関連する判例

【判決の結果】

人民法院は最終的に、苦情後に被告が完全に賠償していなかった差額である243.37元、およびブッキングの差額である1511.37元の三倍の賠償金である合計4777.48元を被告が原告に賠償し、かつ、被告が自社の運営するCtrip APPにおいて、原告のために、同社の既存の「サービス協議書」と「プライバシーポリシー」に同意しない際にも、依然として引き続きサービスを利用することができる選択肢を増加し、または原告のために、Ctrip APPの「サービス協議書」と「プライバシーポリシー」を改定し、ユーザーに対する必要ではない情報の収集および使用の関連内容を除去しなければならない旨を判決した。

【事例の啓示】

ビッグデータを通じた「常連客への差別」は、平等性と信義誠実の原則に違反している。企業は**個人情報を利用して自動化された意思決定を行う際には、アルゴリズムのコンプライアンスを重視し、意思決定の透明性、ならびに結果の公平性および公正性を保証**しなければならず、消費者の嗜好や取引習慣などの特徴に基づき、アルゴリズムを利用して取引価格等の取引条件の面における不合理かつ差別的な待遇等の行為に及んではならない。このほかにも、企業はさらに、APP中の関連「サービス協議書」および「プライバシーポリシー」の審査および改定に注意し、ユーザーからの授権を概括的に要求する行為を根絶しなければならない。

4.3.3 個人情報取扱活動中の個人の権利（「個人情報保護法」から抜粋）

	権利名称	権利内容	根拠
1	**同意撤回権**	個人の同意に基づいて個人情報を取り扱うときは、個人は、自らの同意を撤回することができる。	「個人情報保護法」第15条
2	**知る権利、決定権、制限権、拒否権**	個人は、自らの個人情報の取扱いに対して知る権利と決定権を有し、他者による当該個人の個人情報の取扱いを制限又は拒絶することができる。ただし、法律又は行政法規に別段の定めのあるときは、この限りでない。	「個人情報保護法」第44条
3	**調査・閲覧権、複製権**	個人は、自らの個人情報を個人情報取扱者の下から調査・閲覧・複製することができる。	「個人情報保護法」第45条
4	**その他の個人情報取扱者への移転の請求権**	個人が自らの個人情報の自らが指定した個人情報取扱者への移転を請求した場合において、国家インターネット情報部門の定める条件を満たしていたときは、個人情報の取扱者は、移転のルートを提供しなければならない。	
5	**修正権、削除権**	個人は、自らの個人情報の不正確性又は不完全性に気が付いたときは、個人情報の取扱者に修正又は補完を請求することができる。 個人は、個人情報の削除を請求することができる。	「個人情報保護法」第46条、第47条

4.3.3 個人権利の行使に関連する判例

蘇州貝爾塔数据技術有限会社と伊日克斯慶との間における一般人格権をめぐる紛争案件

（〈 2018 〉蘇0591民初2244号、〈 2019 〉蘇05民終4745号）

【原告と被告】原告：伊氏　　被告：貝爾塔数据技術有限会社

【事例の概要】

被告は啓信宝ウェブサイトの管理者である。当該ウェブサイトは主に、商業コンサルティングサービスを提供しており、公衆は当該ウェブサイトを通じて企業登記、訴訟関連の裁判文書などの情報を照会することができる。2017年に、被告は中国裁判文書網および人民法院公告網というウェブサイトの管理者の授権を経ずに、かつ、原告である伊氏の意見を募らずに、中国裁判文書網上で公開されている三つの裁判文書と、人民法院公告網上で公開されている一つの人民法院による判決書の送達に関する公告文書を啓信宝ウェブサイト上で転載し、誰でも当該ウェブサイト上で上述の文書を検索し、照会することができるようにした。伊氏は上述の文書の当事者であり、上述の法律文書においては、伊氏にかかわる四件の紛争の状況がそれぞれ記述されていた。原告が被告と連絡を取り、文書の削除を要求したところ、被告はこれを削除しなかった。このため、原告は人民法院に訴訟を提起した。

4.3.3 個人情報取扱活動中の個人の権利

当該案件の二審において、人民法院は、次の見解を示した：

本件の文書は、インターネット上において既に合法的に公開されており、被告は公開されているルートに基づいた収集後に、自社の合法的な経営範囲内において顧客に提供し、関連の法的文書を公開しており、これは既に合法的に公開されている情報に対する合理的な使用に属していた。しかし、原告が被告と連絡を取り、文書の削除を要求した後に、被告は依然として中国裁判文書網上で訴訟文書が既に公開されていることを理由とし、本件文書の削除を拒絶しており、これにより原告の個人情報に対する違法な公開と使用の行為を構成していた。**被告が削除を拒絶した行為は、伊氏の既に公開されている情報に対する拡散制御実施の意思表示に背き、合法性・正当性・必要性の原則に違反しており、伊氏の重大な利益に対する影響を構成し、同者の個人情報権益を侵害していたものと**考える。

【判決の結果】

二審において、人民法院は最終的に、次のとおり判決した：被告は、原告の指定した本件の三つの判決文書を削除し、人民元8000元を原告に賠償する。

P74

4.3.3 個人情報取扱活動中の個人の権利

【事例の啓示】

既に公開されている個人情報も、みだりに取り扱うことはできない。企業は既に公開されている個人情報の利用時において、合理的かつ慎重な取扱いの姿勢を保持しなければならない。仮に当該情報の取扱行為が、個人の権益に対して重大な影響を発生させるときは、当該個人の同意を事前に取得しなければならない。このほかにも、**企業はさらに、個人情報の権利行使請求への応答の仕組みの確立および完全化、ならびに個人情報主体の情報に対する調査閲覧・修正・複製・削除の需要への迅速かつ適切な対応に注意**しなければならない。

4.3.4 情報利用の比較

法律	対象	共通点	相違点
サイバーセキュリティ法 データセキュリティ法	データ、重要データ	◆ 適法に利用すること ◆ アクセス権限の設置 ◆ 技術的な措置の採択	社会公徳および論理に適合することの強調
個人情報保護法	個人情報、個人機微情報	◆ 適法に利用すること ◆ アクセス権限の設置 ◆ 技術的な措置の採択	取決めた範囲内に利用すること

P76

4.4.1 情報の越境伝送の前提条件のまとめ

データ	一般的なデータ	セキュリティ評価の不要性
	重要データ	セキュリティ評価の必要性
	個人情報	以下の条件をすべて満たす必要がある。 ①　**法定の手続の実施** ②　**単独の同意** ③　**個人情報保護影響評価の事前の実施**
	個人機微情報	

4.4.2.1 重要データの越境伝送

根拠：「サイバーセキュリティ」第37条、「データセキュリティ法」第31条

原則：重要データを越境伝送する前に、セキュリティ評価を行わなければならない。

「サイバーセキュリティ法」第37条

業務の必要により、確かに国外に提供する必要がある場合は、国家インターネット情報部門が国務院の関係部門と共に制定した規則に従って**セキュリティ評価を行わなければならない**。法律、行政法規に別途規定がある場合は、それに従う。

「サイバーセキュリティ法」第31条

重要情報インフラ施設運営者による、中国国内での運営の過程において収集・発生した**重要データの中国国外への移転に対する安全管理については、「サイバーセキュリティ法」の規定を適用**する。

その他のデータ取扱者による中国国内での運営の過程において**収集・発生した重要データの中国国外への移転に対する安全管理規則**は、国家インターネット情報部門が国務院の関連部門と協議して**制定**する。

4.4.2.2 重要データの越境伝送の比較

法律	重要データの越境伝送	
	CIIO	その他のデータ取扱者
サイバーセキュリティ法	① 中国国内での運営において収集および発生した重要データは、**中国国内に保存**しなければならない。 ② 業務の必要性により、確かに**中国国外に提供する必要がある**ときは、国家インターネット情報部門が国務院の関係部門と共同で制定した規則に従って**セキュリティ評価**を行わなければならない。	規定なし
データセキュリティ法	中国国内における運営の過程において収集・発生した重要データの中国国外への移転に対する安全管理については、「サイバーセキュリティ法」の規定を適用する。	中国国内における運営の過程において収集・発生した重要データの中国国外への移転に対する安全管理規則は、国家インターネット情報部門が、国務院の関連部門と協議して制定する。
自動車データセキュリティの管理に関する若干の規定	① 自動車データ取扱者は、法により自動車業界の重要データを中国国内に保存しなければならない。 ② 業務上の必要性により**中国国外への提供が確かに必要**であるときは、国家インターネット情報部門と国務院の関連部門が共同で実施する**セキュリティ評価を通過**しなければならない。	

4.4 情報の越境伝送

P79

4.4.3.1 個人情報の越境伝送時の法定の手続とは

国家インターネット情報部門が手配するセキュリティ評価への合格

国家インターネット情報部門の規定に従った専門的な機構による個人情報保護認証の実施

国家インターネット情報部門が制定した契約のひな形を用いた中国国外の受領者との契約の締結

個人情報の越境伝送実施の前提となる条件：「個人情報保護法」第38条、第39条および第55条

① 上記の条件のうちのいずれかの充足 ② 個人の単独の同意の取得 ③ 個人情報保護影響評価の実施

4.4 情報の越境伝送

P80

4.4.3.2 個人情報の越境伝送の比較

法律	適用範囲	
	CIIO	その他の個人情報取扱者
サイバーセキュリティ法	① 中国国内での運営において収集および発生した個人情報は、**中国国内に保存**しなければならない。 ② 業務の必要により、確かに**中国国外に提供する必要がある**ときは、国家インターネット情報部門が国務院の関係部門と共に制定した規則に従って**セキュリティ評価**を行わなければならない。	規定なし
個人情報保護法	CIIOと国家インターネット情報部門の定める数量に達している個人情報の取扱者は、 ① 中国国内において収集され、または発生した個人情報を中国国内に保存しなければならない。 ② 中国国外への提供が確かに必要なときは、国家インターネット情報部門のセキュリティ評価に合格しなければならない。	以下の条件をすべて満たす必要がある。 ① 法定の手続の実施 ② 単独の同意 ③ 個人情報保護影響評価の事前の実施
自動車データセキュリティの管理に関する若干の規定	① 10万人以上の個人情報は、自動車業界の重要データに該当する。 ② 自動車業界の重要データは、中国国内に保存しなければならない。 ③ 業務上の必要性により**中国国外への提供が確かに必要**であるときは、国家インターネット情報部門と国務院の関連部門が共同で実施する**セキュリティ評価を通過**しなければならない。	

4.4.4 その他の情報の越境伝送

法律	対象	内容
データセキュリティ法	データ、重要データ	第36条 国内の組織・個人は、中国の主管機関による審査認可を経ずに、国外の司法又は法執行機構に対して、中国国内に保存されているデータを提供してはならない。
個人情報保護法	個人情報、個人機微情報	第38条第2項 中華人民共和国の締結又は参加した国際的な条約・協定が、中国国外への個人情報の提供に対する条件等を定めていたときは、その規定に従って執行することができる。 第41条 中華人民共和国の主管機関の認可を経ずに、個人情報の取扱者は、中国国内に保存された個人情報を外国の司法機関又は法執行機関に提供してはならない。

五、実務への対応の方法

5.1 全体像

P83

◆データ（個人情報を含む、以下は同じ）セキュリティガバナンスのキーポイント：

「データの対象化」→「種々の主体による共同の参画」→**「発展と安全の両立」**

データの対象化

データの全ライフサイクルの把握	具体的な業務の状況への照準の設定	データセキュリティの脅威およびリスクの認識

↓

種々の主体による共同の参画

共同の参画による統治の枠組みの構築	各当事者の責任の明確化	データセキュリティに関する各当事者の共通の認識の統一化

↓

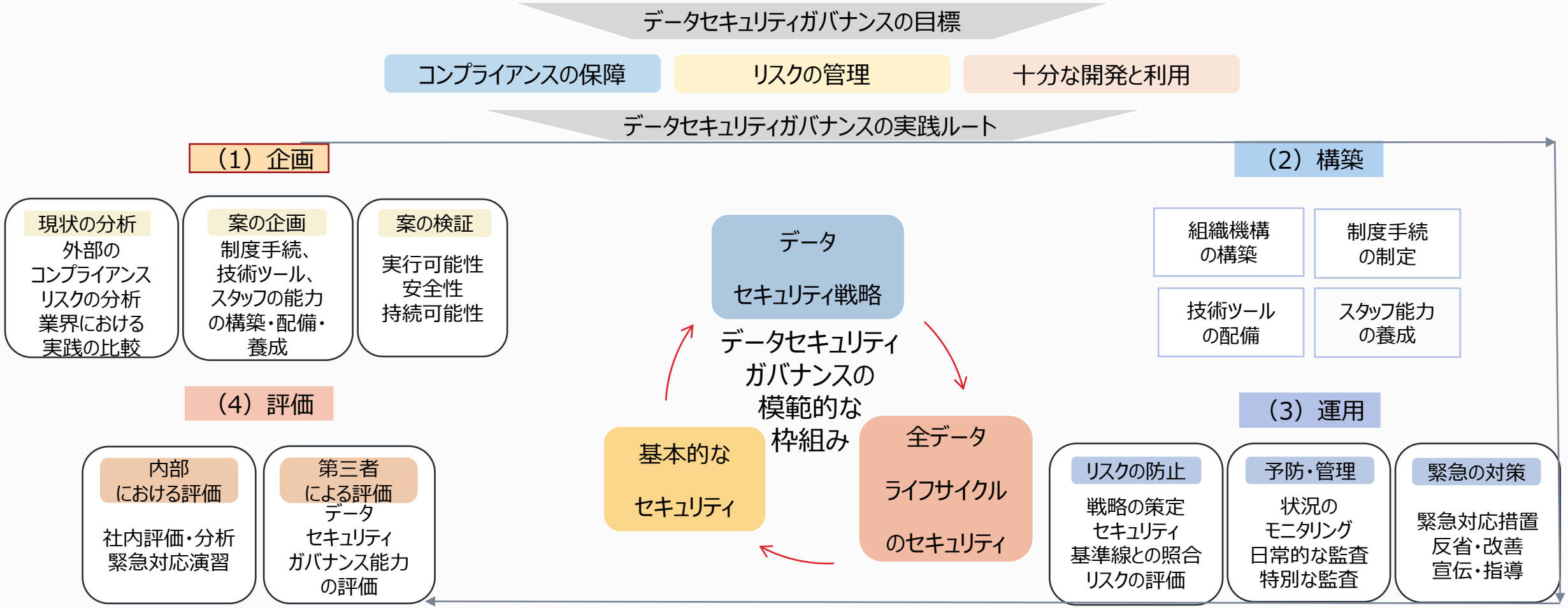
発展性と安全性の両立

データの開発・利用および産業の振興に向けたテータセキュリティ促進の方向性の堅持	データセキュリティを通じたデータの開発・利用および産業の振興に対する保障の方向性の堅持

5.1 全体像

P84

◆**模範的な枠組み**に従ったデータセキュリティガバナンスの**実践**の展開、**コンプライアンスとリスク管理**を前提とするデータの**開発利用**の実現、事業の持続的かつ健全な発展の保障、発展性と安全性の両立の促進



5.1 全体像

P85

◆データセキュリティは、データセキュリティガバナンスの目標である。模範的な枠組みは、データセキュリティガバナンスの参照案である。企業は参照案の構築を通じて効果的な目標の管理を実現することができる。

- トップダウン設計時における**目標の設定、チームの編成**
- 収集、移転、保存、使用、共有、削除などの各段階を**目安にした管理ポイントの**設定
- ガバナンスシステム全体の**共通の**要求
- 資源の**有効な統合**の実現可能性を模索

5.2 具体的な対応策

P86

管理制度の樹立、完全化

- ◆ 企業内部の実状の確認
- ◆ 法による管理制度の樹立、完全化
- ◆ 法によるセキュリティインシデント緊急対応プランの作成、完全化など

責任者と管理機構の選定

- ◆ 管理責任者の選定（DPOなど）
- ◆ 管理機構と管理体制の制定

具体的な実務ガイドラインの制定

- ◆ 収集、保管、使用などに関する基本原則の制定
- ◆ 企業内部における実施細則の策定、完全化など

教育研修の定期的な実施

- ◆ 研修制度の強化
- ◆ 規則違反時の責任等
- ◆ 社内教育研修の定期的な実施、関連記録の適切な保存

法令上の特別な義務の履行

- ◆ 自社から重要情報インフラ運営者や重要情報取扱者などへの当否の確認
- ◆ 特別な義務の徹底的な履行（もしあれば）

5.3 必要な対応内容

P87

法律	対応策の内容						
	安全管理制度、実務規程の制定	責任者の確定	技術的措置の実施	セキュリティインシデントの監視、報告	データの分類、暗号化	社内教育研修の実施	セキュリティの評価
サイバーセキュリティ法	○	○	○	○	○	一般：× CIIO：○	○ （越境伝送評価）
データセキュリティ法	○	○	○	○	○	○	○ （重要データ取扱活動リスク評価）
個人情報保護法	○	○ （規定数に達した個人情報取扱者のみ）	○	○	○	○	○ （個人情報保護影響評価）

5.4 対応方法

P88

◆実状の確認、データマッピング

当事務所が別件で作成した調査アンケートの実例

データセキュリティに関するチェックリスト

1 基本状況チェック

1.1 基本情報

正式名称	●●●●有限公司(以下「貴社」)
所属業種	●●●●業
在籍人数	共に【 】名 そのうち、正社員【 】名、派遣社員【 】名、日本から出向される方【 】名、その他【 】名。
日常業務	業務の概要について、教えてください。 1. ●●●● 2. ●●●● 3. ●●●●
IT 管理	
現地公式サイト	

1.2 日常の業務においてインターネットを使用(または運営)しているか否か？(複数選択可能)

1.2 日常の業務においてインターネットを使用(または運営)しているか否か？(複数選択可能)

☑ ①自社のウェブサイトがあり、インターネット情報サービス届出を行っている。
☑ ②ウェブサイトプラットフォームを確立し、付加価値電信経営許可証を取得している。
☑ ③内部において LAN を確立している。
☑ ④産業制御システムを通じて生産を管理している。
☑ ⑤インターネットアクセスサービスを提供している。
☐ ⑥インターネットを使用(または運営)していないけれども、インターネット関連製品またはサービスを提供している。
☐ ⑦インターネットを使用せず、インターネットにも関連性がない。

1.3 貴社が使用又は運営しているシステムの概要を教えてください。

概要として、かかるシステムの名称、役割、想定する利用者、取扱うデータの内容を教えていただければと存じます。

1.【A システム】

2.【B システム】

3.【C システム】

5.4 対応方法

P89

◆データマッピングによる結果のまとめ

当事務所が別件で作成した
調査報告書の実例

データセキュリティーに関する調査報告書

標題の件につきまして、ご提供いただいた関連情報に基づき、弊事務所における検討を経て、以下のとおりご報告いたします。ご検討のほどお願い申し上げます。

1　調査全般

弊職らは、●●●●有限公司北京駐在員事務所（以下「**貴事務所**」という）からのご依頼に従い、貴事務所を対象とするデータセキュリティーに関する専門的な調査（以下「**本件調査**」という）を実施しました。本件調査の目的と実施方法は以下のとおりです。

(1) 調査目的

本件調査を通じて、下記の目的を達成したく存じます。

5.4 対応方法

P90

◆データマッピングの結果に基づく対応

各種の管理制度の制定および変更

必要となる社内規程は、下表のとおり想定される

社内規程の名称
➢ サイバーセキュリティに関する管理規程
➢ サイバーセキュリティ等級保護に関する管理規程
➢ データセキュリティ規程、データセキュリティ細則、データセキュリティガイドライン
➢ 個人情報保護取扱規程、個人同意書、プライバシーポリシー
➢ サイバーセキュリティインシデント対応プラン、データセキュリティインシデント対応プラン、個人情報セキュリティインシデント対応プラン
➢ 個人情報・重要データ越境伝送規程など

六、Q&A

中国の個人情報保護法と、
日本の個人情報保護法と 、
欧州のGDPRとの間の違いについて
教えてください。

6.1 Q&A

P93

※令和二年法律第四十四号。R02.06.12 公布 / R04.04.01 施行

	中国の「個人情報保護法」	日本の「個人情報の保護に関する法律」※	欧州のGDPR
適用範囲	中国国内＋域外適用	日本国内＋域外適用＋適用例外	域内適用＋域外適用（属人主義）
個人機微情報	同意の取得後における取扱いの可能性+制限条件の付加	同意の取得後における収集の可能性+例外的な状況	原則として禁止 +例外的な状況
未成年者への特別な保護	満14歳を基準とする	規定なし（ただし、個人情報保護委員会が制定したガイドラインに関連内容がある）	満16歳を基準とする
越境伝送	① 情報の取得・発生国家における当該情報保存義務の規定：あり ② 法定の手続 +単独の同意　+リスクの評価	①情報の取得・発生国家における当該情報保存義務の規定：なし ②制限条件の規定	①情報の取得・発生国家における当該情報保存義務の規定：なし ② ホワイトリスト +適切な保護措置の採択
個人の権利	知る権利、取扱制限権、取扱拒絶権、取得・移転権など	取扱拒絶権、修正・追加権など	知る権利、取扱制限権、取扱拒絶権、取得・移転権など
罰金	最高で人民元5000万元、または前年度の売上高の5%に相当する金額（両者のうち高いほうを賦課）	最高で日本円1億円	最高で2000万ユーロ、または前年度のグローバル総売上高の4%に相当する金額（両者のうち高いほうを賦課）

中国のデータセキュリティ法と
輸出管理法との間の関係性について
教えてください。

◆「データセキュリティ法」第25条

国は、国家の安全・利益の保障、国際的な義務の履行に係り、または規制対象品目に該当するデータに対し、輸出管理を法により実施する。

◆「輸出管理法」第2条2項

管理品目には、当該品目にかかわる技術資料などのデータが含まれる。

◆「輸出管理法」第12条

次の状況に属する品目の貨物・技術・データは、輸出許可の申請が必要となる。

リスト規制　⇒　中国輸出禁止輸出制限技術目録（2020年改定版）

キャッチオール規制　⇒　輸出管理リストに掲載された管理品目および臨時管理品目以外の貨物・技術・サービスに、同条の定めるリスク（すなわち、1、国家の安全・利益に対する脅威　2、大規模殺傷性武器およびその運輸・搭載手段の設計・開発・生産・利用への使用　3、テロリズム目的への使用）が存在しているおそれのある状況を輸出事業者が知り、もしくは知り得べきであり、または、輸出管理部門の通知を受けたとき。

P96

サイバーセキュリティ等級保護の
早期取得の重要性について
教えてください。

6.3 Q&A

P97

◆「サイバーセキュリティ法」第21条

ネットワーク運営者は、サイバーセキュリティ等級保護制度の要求に従って安全保障義務を履行しなければならない。

◆「データセキュリティ法」第27条

インターネット等の情報ネットワークを利用したデータの取扱活動を行うときは、サイバーセキュリティ等級保護制度に従って上記のデータセキュリティ保障義務を履行しなければならない。

◆「自動車データセキュリティの管理に関する若干の規定」第5条

インターネット等の情報ネットワークを利用して自動車データ取扱活動を行う場合、サイバーセキュリティ等級保護等の制度を実施し、自動車データの保護を強化し、法によりデータセキュリティ義務を履行しなければならない。

等級保護の取得は、既に「データセキュリティ法」における法定の義務の一環となっていることから、その早期取得の重要性は、更に高まっている。

特に、自動車業界など特定分野の企業に対しては、早期の取得が推奨されている。

CIIOに該当するか否かというのは
どのように判断されるのですか？

6.4 Q&A

P99

「重要情報インフラセキュリティ保護条例」においては、CIIOの具体的な認定規則は規定されていない。CIIOの認定について、当面の間は、以下の方法を採用して、予備的な判断を行うことができる。

◆予備的な自己判断：

① 所属業界　② 自らの業界における重要度、自らの破壊への遭遇後の危険性

◆予備的判断の実施の専門機構または法律事務所への委託

「重要情報インフラセキュリティ保護条例」第8条、第9条

本条例の第 2 条の定める重要な業界・分野の主管部門と管理監督部門は、重要情報インフラセキュリティ保障業務の職責を負担する部門（以下「保障業務部門」という。）とする。

保障業務部門は、管轄する業界と分野の実状を踏まえて重要情報インフラに対する認定の規則を制定し、国務院公安部門に届出を行う。

P100

サイバーセキュリティ法、データセキュリティ法、
個人情報保護法の諸規制を踏まえた上で、
製造、医療、金融、インターネットなど
の業界に属する企業にとっての
それぞれの注意点について
教えてください。

6.5 Q&A

P101

法律/業界	製造	医療	金融	インターネット
サイバーセキュリティ法	◆ サイバーセキュリティの等級保護 ◆ インダストリアルインターネットの保護 ◆ IOTの対応	◆ 医療システムの等級保護	◆ CIIOの認定 ◆ 金融機構システムの等級保護	◆ 超大型インターネットプラットフォームのCIIOの認定 ◆ サイバーセキュリティの等級保護
データセキュリティ法	◆ 工業データの分類・分級 ◆ 自動車業界における重要データの認定	◆ 医療データの分類・分級	◆ 金融データの分類・分級 ◆ 金融業の重要データの取扱い	◆ データセキュリティ ◆ アルゴリズム運用の適法化
個人情報保護法	◆ B2C類の個人情報の収集・保存・利用	◆ 個人機微情報の取扱い ◆ 死亡者の個人情報の保護	◆ 個人機微情報の取扱い ◆ 個人情報の越境伝送	◆ 自動化された意思決定 ◆ 超大型インターネットプラットフォームの個人情報保護上の特別な義務

6.6 Q&A

P102

「個人情報保護法」の下での
従業員個人情報の取扱上の注意点について
教えてください。

6.6 Q&A

P103

◆従業員個人情報のマッピング

- ✓ 従業員の同意を要せずに取り扱うことのできる従業員の個人情報（「個人情報保護法」第13条第1項第（2）号）と、従業員の同意を取得する必要があり、その後に初めて取り扱うことのできる個人情報との間における明確な分離
- ✓ 従業員を認識することのできる個人機微情報（指紋、顔情報などを含む生体認証情報、健康情報、銀行口座情報など）への注意
- ✓ 会社の業務における特別な状況の存在の把握（共同の取扱い、取扱委託、第三者への提供など）

◆従業員の個人情報の保護にかかわる制度の制定

- ✓ 関連の保護制度、および個人情報セキュリティインシデント緊急対応プランの制定
- ✓ 従業員による関連の権利（同意撤回権、取扱拒絶権など）の行使に関する制度の制定

◆従業員の個人情報の越境伝送時における①関連手続の履行　+② 従業員の単独の同意の取得 +③ 事前の評価の実施の義務の履行

◆必要な技術的措置の採択、個人情報のセキュリティの確保

金诚同达律师事务所

P104

主管部門の現場調査への対応策として、
何を行うことができますか？

6.7 Q&A

P105

冷静沈着かつ専門的な対応

政府の調査官への対応：

- 指示に従った行動
- 礼儀正しさ、友好的な姿勢
- 従業員から調査官への意図的な、または過失による妨害の回避
- 調査官の懸念事項に対する把握を目的とする可能な限り多くの情報（調査事項など）の調査官からの入手
- 調査への全面的な協力の姿勢の強調
- 調査官の質問に対する正直な応答、調査官との会話内容の記録、または（記録が不可の場合における）ヒアリング終了後の時宜を得た記録（ヒアリング中の関連内容を回想し、質問と回答の具体的な内容を書き留めておくことが必要）

北京本部

住　　所：北京市朝陽区建国門大街1号国貿大厦（三期）A座10層

郵便番号：100004

信用を守ること金石のごとく誠なり
奮起向上の意志を奨励し
同刻に到達す

守信金誠、励志同達

ご清聴ありがとうございました。

金诚同达律师事务所