# 中国サイバーセキュリティ法の改正について

－総体国家安全観を貫徹したサイバー強国建設の推進
－AI 関連の重要技術開発を支援等、第 15 次 5 ヵ年計画の策定に関する中共中央の建議を具体化
－罰則の大幅な強化、域外適用の対象範囲の拡大も
－データ関連法制との連動によるガバナンス強化

2025.11.27
CISTEC 事務局

10 月 28 日、全国人民代表大会において、中華人民共和国サイバーセキュリティ法が改正[1]された（2026 年 1 月 1 日施行）。

今回の改正について、ネットワーク侵入やサイバー攻撃、違法情報の拡散などが頻発していることに触れ、「ネットワークの運用安全、ネットワーク製品・サービスの安全、ネットワーク情報安全を**脅かす行為に対する法的責任を重点的に整備**し、**処罰の強化**、法律の**域外適用状況の拡大**を図るとともに、データセキュリティ法、個人情報保護法などのネットワーク分野関連法律との連携を強化」し、人工知能（AI）のガバナンスと発展促進のニーズに応え、「国が AI 基礎理論研究やアルゴリズムなどの重要技術開発を支援し、訓練データ資源や計算能力などのインフラ整備を推進し、AI 倫理規範を整備し、リスク監視評価と安全監督を強化し、AI の応用と健全な発展を促進し、革新的なサイバーセキュリティ管理手法を支援し、人工知能などの新技術を活用してサイバーセキュリティ保護レベルを向上させる」[2]としている。

サイバーセキュリティ法は 2016 年 11 月に公布[3]（2017 年 6 月に施行）されて以降、初めての改正となる。本法の改正案は、2022 年 9 月に意見公募[4]が行われ、その後、本年 3 月に第 2 次意見募集稿が公表[5]されていた。

---

[1] 全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定（全国人民代表大会サイト 2025 年 10 月 28 日）別添 1※機械翻訳
http://www.npc.gov.cn/npc/c2/c30834/202510/t20251028_449048.html

[2] 完善网络安全法律责任 回应人工智能治理发展需要（全国人民代表大会サイト 2025 年 10 月 29 日）
http://www.npc.gov.cn/npc/c2/c30834/202510/t20251029_449086.html

[3] 中华人民共和国网络安全法（全国人民代表大会サイト 2016 年 11 月 7 日）
http://www.npc.gov.cn/zgrdw/npc/xinwen/2016-11/07/content_2001605.htm 別添 2※CISTEC 仮訳

[4] 中華人民共和国サイバーセキュリティ法〉修正に関する決定（意見募集稿）》の意見公開募集に関する通知（CISTEC 仮訳）https://www.cistec.or.jp/members/z1905sokuho/20220915.pdf

[5] 关于公开征求《中华人民共和国网络安全法（修正草案再次征求意见稿）》意见的通知（中華人民共和国国家インターネット情報弁公室 2025 年 3 月 28 日）https://www.cac.gov.cn/2025-03/28/c_1744779434867328.htm

## 1．概要

### ① 総体国家安全観を貫徹したサイバー強国建設の推進（第 3 条）

サイバーセキュリティ業務に関し、中国共産党の指導を堅持し、総体国家安全観を貫徹し、サイバー強国の建設を推進する旨が規定された[6]。

10 月 20 日～23 日に開催された中国共産党第 20 期中央委員会第 4 回全体会議（4 中全会）の最終日に発表されたコミュニケ[7]（以下抜粋）において、**サイバー強国の建設を加速**する旨が提唱されている。

> 全会では、現代的な産業体系を構築し、実体経済の基盤を固め、強化することを提唱した。経済発展の重点を実体経済に置き、知能化・グリーン化・融合化の方向を堅持し、製造強国・品質強国・宇宙強国・交通強国・**サイバー強国の建設を加速**し、製造業の適正な比重を維持し、先進製造業を中核とする現代的な産業体系を構築する。伝統産業の最適化・高度化を図り、新興産業と未来産業を育成・拡大し、サービス業の高品質・高効率な発展を促進し、現代的なインフラ体系を構築する。

### ② AI 重要技術開発支援・インフラ整備の推進・AI に関する監督等の強化等（第 20 条）

AI 重要技術の開発支援やインフラ整備の推進、AI に関する監督等の強化など、AI に関する規定として、「国は**人工知能の基礎理論研究及びアルゴリズム等の重要技術開発を支援**し、**訓練データ資源、計算能力等のインフラ整備を推進**し、人工知能倫理規範を整備し、リスク監視評価及び安全監督を強化し、人工知能の応用と健全な発展を促進する。国はサイバーセキュリティ管理方法の革新を支援し、人工知能等の新技術を活用して、サイバーセキュリティ保護水準の向上を図る」旨が規定された。

10 月 23 日、中国共産党第 20 期中央委員会第 4 回全体会議（4 中全会）において、「国民経済・社会発展第 15 次 5 ヵ年計画の策定に関する中共中央の建議」が採択され、AI の基礎理論の支援、AI 科学研究のパラダイムシフトを牽引、AI ガバナンスの強化、関連法規の充実等を触れている。

---

[6] 国家安全法第 25 条においてセキュリティ管理の規定あり。
中华人民共和国国家安全法（主席令第二十九号）（中華人民共和国中央人民政府サイト 2015 年 7 月 1 日）
https://www.gov.cn/zhengce/2015-07/01/content_2893902.htm
第 25 条　国家はネットワークと情報のセキュリティ保障体系を建設し、ネットワークと情報安全の保護能力を向上させ、ネットワークと情報技術のイノベーション研究と開発応用を強化する；ネットワーク管理を強化し、サイバー攻撃、ネットワーク侵入、ネットワーク機密窃取、違法な有害情報の散布などのサイバー違法犯罪行為から防備し、これを防止し法によって懲罰し、国家のサイバースペースの主権、セキュリティと発展の利益を擁護する。

[7] 中国共产党第二十届中央委员会第四次全体会议公报（中華人民共和国中央人民政府サイト 2025 年 10 月 23 日）https://www.gov.cn/yaowen/liebiao/202510/content_7045444.htm

国民経済・社会発展第 15 次 5 ヵ年計画の策定に関する中共中央の建議[8]

**四　ハイレベルの科学技術の自立自強を加速し、新質生産力の発展をリードする。**

中国式現代化は科学技術の現代化によって支える必要がある。新たな科学技術革命と産業変革の歴史的チャンスをつかみ、教育強国・科学技術強国・人材強国の建設を統一的に計画し、国のイノベーション体系全体の効果を高め、自主イノベーション能力を全面的に向上させ、科学技術発展の上位を占め、新質生産力[9]を不断に生み出す。

（14）人工知能（AI）などのデジタル・インテリジェンスのイノベーションを急ぎ、基礎理論と核心技術を突破し、計算力・アルゴリズム・データなどの効果的な供給にいっそう力を入れる。**「AI＋」行動を全面的に実施し、AI で科学研究のパラダイムシフトを牽引**し、AI と産業発展、文化建設、民生保障、ソーシャル・ガバナンスとの結合を強化し、AI の産業応用において上位を占め、全方位的に各業界を後押しする。**AI ガバナンスを強化し、関連法律法規・政策制度・応用規範・倫理準則を充実**させる。監督管理を改善し、プラットフォーム経済の革新、健全な発展を推し進める。

### ③ ネットワークプロバイダによる個人情報の処理（第 42 条）

ネットワークプロバイダ[10]が個人情報[11]を処理する場合、「サイバーセキュリティ法及び中華人民共和国民法典、中華人民共和国個人情報保護法等の法律・行政法規の規定を遵守しなければならない」旨の規定が追加され、データ関連法規との整合性が図られている。

---

[8] 国民経済・社会発展第 15 次 5 ヵ年計画の策定に関する中共中央の建議（全文）（新華網 2025 年 10 月 28 日）
https://jp.news.cn/20251028/6cf06607daee4220a9a5b8c6ea51916f/c.html

[9] 2024 年 7 月、中国共産党第 20 期中央委員会第 3 回全体会議（3 中全会）における「改革をいっそう全面的に深化させ中国式現代化を推進することに関する中共中央の決定」において、次世代情報技術、人工知能（AI）、航空宇宙、新エネルギー、新素材、ハイエンド設備、バイオ医薬、量子技術など戦略的産業の発展につながる政策とガバナンス体系を整備し、新興産業の健全で秩序ある発展を導くとされている。
「改革をいっそう全面的に深化させ、中国式現代化を推進することに関する中共中央の決定」（全文）（新華網サイト 2024 年 7 月 21 日）
https://jp.xinhuanet.com/20240721/938b8afe526441a28b5242768bc3edc0/ebb98d461de94917878d336dac5dc962.pdf

[10] ネットワークの所有者・管理者とネットワークサービスの提供者（ネットワークサービスプロバイダ）を指す（第78条）。

[11] 電子あるいはその他の方式で記録した単独で、あるいはその他の情報と結び付けて個人の身分を識別することのできる各種情報を指し、これには自然人の姓名、出生期日、身分証番号、個人生体認証情報、住所、電話番号などが含まれる。（第78条）。
※個人情報保護法では、識別可能な自然人に関する各種情報のうち匿名化処理された情報は含まない（第4条）、とされている。

なお、従前より、ネットワークプロバイダに関して、個人情報の収集や使用、提供等の取扱いなどの規定はいくつか存在[12]していた。重要情報インフラ[13]運営者については、第 39 条（旧第 37 条）において個人情報の国内保存義務や国外提供時の安全評価義務が規定されていた。

| |
|---|
| 第37条　最重要情報インフラの運営者が中華人民共和国国内の事業のなかで収集・作成した個人情報と重要データは国内で保存しなければならない。業務の必要により、確かに国外に提供しなければならないものは、国家のネットワーク情報部門が国務院の関連部門と共同で制定した規則に基づいて安全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ものは、その規定に基づく。 |

**④ 罰則強化**

（イ） ネットワークプロバイダにおけるサイバーセキュリティ保護義務[14]違反

1 万元以上 5 万元以下の罰金【新設※従来は是正命令・警告のみ】

※是正拒否、危害等を招いた場合、5 万元以上 50 万元以下の罰金【改正前の 5 倍】

直接の責任者に対し、1 万元以上 10 万元以下の罰金【改正前の 2 倍】

（ロ） 重要情報インフラ運営者におけるサイバーセキュリティ保護義務[15]違反

5 万元以上 10 万元以下の罰金【新設※従来は是正命令・警告のみ】

※是正拒否、危害等を招いた場合の罰則（10 万元以上 100 万元以下）は変更（改正）なし。

（ハ） 上記（イ）及び（ロ）の行為により、重大な危害等をもたらした場合

---

[12] サイバーセキュリティ法第 42 条～第 47 条

[13] 重要情報インフラとは、**公共通信と情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政務などの重要産業と分野、およびひとたび破壊、機能喪失、あるいはデータ漏えいなどに遭ったならば、国家安全、国の経済と人民の生活、公共の利益に深刻な危害が加えられる恐れのあるもの**をいい、国はサイバーセキュリティ等級保護制度に基づき、重点保護を実施する（第 33 条)。

[14] ネットワークプロバイダのセキュリティ保護義務

内部コンプライアンス構築（セキュリティ管理システム及び運用規程、責任者の決定)、サイバー攻撃、ネットワーク侵入等の防止措置、システム運用状態のモニタリング、重要データのバックアップ、暗号化等の対策等（第 23 条)、インシデント対応マニュアルの策定等（第 27 条）

[15] 重要情報インフラ運営者のセキュリティ保護義務

重要情報インフラの建設に際しセキュリティ技術措置の計画・構築することの保証（第 35 条)、専門セキュリティ管理機関及びセキュリティ管理責任者の設置、責任者等の身元調査の実施（第 36 条)、ネットワーク製品及びサービスの調達に当たり提供者と秘密保持契約を締結等（第 38 条)、ネットワークセキュリティ及びリスクの検査・評価（年に一度)、結果を関連当局へ報告（第 40 条）

・**大量のデータ漏洩**、重要情報インフラの**部分的な機能喪失等の重大な危害**の場合、50万元以上200万元以下の罰金、直接の責任者には5万元以上20万元以下の罰金【新設】
・重要情報インフラの**主要機能喪失等の特に重大な危害**の場合、200万元以上1000万元以下の罰金、直接の責任者に対し20万元以上100万元以下の罰金【新設】

（ニ） ネットワーク製品及びサービスの提供者や個人及び組織が発信する情報等に悪意のあるプログラムの設定の禁止の義務違反等

ネットワーク製品、サービスの提供者や個人及び組織が発信する情報等に悪意のあるプログラムの設定の禁止の義務（第24条第1項[16]及び第2項、第50条第1項[17]）に違反して上記（ハ）に掲げる重大な危害等をもたらした場合、同規定に基づき処罰する。【新設】

（ホ） ネットワーク重要設備、ネットワークセキュリティ専用製品の販売及び提供の停止、違法所得の没収（第63条）

ネットワーク重要設備及びネットワークセキュリティ専用製品[18]は国家標準の強制的な要件に基づき資格を有する機関によるセキュリティ認証に合格又はセキュリティ検査の要件適合を得た後にのみ販売又は提供することができる旨の規定（第25条）に違反した場合、販売及び提供の停止命令・違法取得の没収の罰則が新設された。

| |
|---|
| 第63条　本法第25条の規定に違反し、セキュリティ認証・セキュリティ検査を受けていない、セキュリティ認証不合格、セキュリティ検査基準不適合のネットワーク重要設備及びネットワークセキュリティ専用製品を販売又は提供した者は、関係主管部門により販売又は提供の停止を命じられ、警告を与えられ、違法所得を没収される。違法所得がない場合または違法所得が10万元未満である場合は、2万元以上10万元以下の罰金 |

---

[16] ネットワーク製品、サービスは関連する国家標準の強制的要求に符合していなければならない。ネットワーク製品、サービスの提供者は悪意のあるソフトウェアを設置してはならない。；そのネットワーク製品、サービスにセキュリティ上の欠陥、脆弱性などのリスクを発見したならば、速やかに救済措置を講じ、規定に基づいて速やかにユーザーに告知し、関連主管部門に報告しなければならない。

[17] **いかなる個人・組織であろうとも**、発信する電子情報、提供するアプリケーションソフトウェアに悪意のあるソフトウェアを組み込んではならず、法律・行政法規で発布あるいは発信を禁止する情報を含めてはならない。

[18] 关于调整《网络关键设备和网络安全专用产品目录》的公告（中華人民共和国中央人民政府サイト 2023年7月3日）https://www.gov.cn/zhengce/zhengceku/202307/content_6889847.htm

ネットワーク重要設備としてルーター、スイッチ、サーバー等4種類が、ネットワークセキュリティ専用製品としてデータバックアップ復旧製品、ファイアウォール、侵入検知システム（IDS）等34種類が列挙。

（参考）关于调整网络安全专用产品安全管理有关事项的公告（中華人民共和国中央人民政府サイト 2023年4月12日）https://www.gov.cn/zhengce/zhengceku/2023-04/18/content_5751982.htm

を併科する。違法所得が 10 万元以上の場合は、違法所得の 1 倍以上 5 倍以下の罰金を併科する。情状が重い場合は、関連業務の停止、営業停止・改善命令、関連業務許可証の取消しまたは営業許可証の取消しを命ずることができる。法律・行政法規に別段の定めがある場合は、その規定による。

（ヘ） システム脆弱性、コンピュータウイルス、サイバー攻撃、ネットワーク侵入等のサイバーセキュリティ情報を社会に発布した場合等（第 65 条）

1 万元以上 10 万元以下の罰金【新設※従来は是正命令・警告のみ】

※是正拒否、情状が重い場合、10 万元以上 100 万元以下の罰金【改正前の 10 倍】

直接の責任者に対し、1 万元以上 10 万元以下の罰金【改正前の 2 倍】

※上記（ハ）に掲げる重大な危害等をもたらした場合、同規定に基づき処罰【新設】

（ト） 重要情報インフラ運営者が安全審査を経ていない・安全審査に合格していないネットワーク製品及びサービスを使用した場合（第 67 条）

是正命令及び国家安全への影響の排除命令【新設※従来は使用停止命令のみ】

（チ） ネットワークプロバイダによるユーザーが発布した情報管理等に関する義務違反（第 69 条）

ネットワークプロバイダは、ユーザーが公表又は発信が禁止される情報を扱っている場合に当該情報の伝送を停止し、消去等の措置を講じ、拡散を防止する措置等を講ずること（第 49 条)、国家ネットワーク関連部門からユーザーの発信を停止するよう要求され消去等の措置等を講ずること（第 52 条）に違反した場合、(従来の是正命令等に加えて）5 万元以上 50 万元以下の罰金の罰金【新設※従来は是正命令・警告のみ】

是正拒否、情状が重大である場合、50 万元以上 200 万元以下の罰金【下限額が改正前の最大 10 倍】

※特に重大な影響又は特に重大な結果を生じた場合、200 万元以上 1000 万元以下の罰金等【新設】

（リ） 重要情報インフラの運営者が個人情報や重要データを国外に保存又は国外に提供した場合（第 71 条）

従来、サイバーセキュリティ法において、独自に罰則（是正命令・違法所得の没収・罰金）が規定されていたが、今般の見直しにより、関連法規（個人情報保護法等）に基づき、処理、処罰される旨の規定に修正された。

（ヌ） 情状酌量・処罰軽減、免除規定（第 73 条）

「本法の規定に違反した場合であっても、『中華人民共和国行政処罰法』に定める情状酌量の余地がある、処罰を軽減する、または処罰を免除する事情があるときは、その規定に基づき情状酌量し、処罰を軽減し、または処罰を免除する。」旨が規定された。

（ル） 国外の機関、組織及び個人等に対する域外適用の強化（第 77 条）

従来より国外の機関等に対する域外適用の規定は存在していた（以下、第 75 条）。従来は法的責任の対象として、**重要情報インフラ**に危害を加える活動に従事し、**深刻な悪影響をもたらせた場合**とされていた。

> 第 75 条　国外の機構・組織・個人が攻撃・侵入・妨害・破壊などの中華人民共和国の**最重要情報基礎施設（インフラ）に危害を加える活動に従事**し、**深刻な悪影響をもたらせたならば**、**法に基づいて法律責任を追及**する。国務院の公安部門と関連部門は当該機構・組織・個人に対して財産を凍結する、あるいはその他の必要な制裁措置をとることを決定することもできる。

今般の改正では「国外の機関、組織、個人が**中華人民共和国のネットワーク安全に危害を加える活動に従事した場合、法的責任を追及**する。重大な結果を招いた場合、国務院公安部門及び関係部門は、当該機関、組織、個人に対し、財産の凍結その他の必要な制裁措置を講じることができる。」とされており、その対象は**重要情報インフラから中国のネットワークの安全に危害を加える活動に従事した場合に法的責任が追及される形に修正**がなされている。**重要情報インフラのみならず、ネットワーク全般**にその対象が拡大されている。

> 【改正後】
> 第 77 条　国外の機関、組織、個人が、中華人民共和国の**ネットワーク安全に危害を加える活動に従事した場合、法に基づき法的責任を追及**する。深刻な結果を招いた場合、国務院公安部門及び関係部門は、当該機関、組織、個人に対し、資産凍結その他の必要な制裁措置を講じることができる。

## 2．まとめ

サイバーセキュリティ法は 2016 年に制定され、データセキュリティ法（2021 年制定）及び個人情報保護法（2021 年）と共にデータ 3 法としてデータ関連法制の一つと位置付けられ、これらの規制は相まって運用されている。昨年 9 月には、ネットワークデータセキュリティ管理条例[19]が制定され（本年 1 月に施行）、データ 3 法の実施規則も公表されている。

[19] 中华人民共和国国务院令第 790 号（中華人民共和国中央人民政府サイト）
https://www.gov.cn/zhengce/content/202409/content_6977766.htm

今般の改正では、前述したように、罰則の内容を大幅に拡大し、**ネットワークプロバイダ、重要情報インフラ運営者、ネットワーク重要設備やサイバーセキュリティ専用製品の販売者等の様々なステークホルダー**に対する規制が強化されている。

特にネットワークプロバイダ及び重要情報インフラ運営者に対する運行上の安全に関する一般的な義務規定違反について、従来は、是正命令・警告に留まっていたもの（是正拒否やネットワークの安全を脅かす等の場合に罰則という構図）が、改正法ではこれと並行して罰則を科すことができる形に修正がなされており、規制遵守の厳格化の姿勢が強く見受けられる。

また、**外国企業も関係する可能性のある、ルーターやスイッチ等のネットワーク重要設備等の販売者等**に対し、セキュリティ認証等を受けていない場合、**販売停止命令や違法所得の没収、情状が重い場合は業務停止、営業停止、営業許可証の取り消し命令等の罰則も新設**されている（これに関連し、**これらの製品を使用した重要情報インフラ運営者**に対する**是正命令及び国家安全への影響の排除命令も新設**。）。

さらに、**域外適用の拡大**として、国外の機関、組織、個人が**中華人民共和国のネットワーク安全を脅かす活動に従事した場合に法的責任を追及**するなど、規制対象範囲が大幅に拡大している。

このように、中国ではサイバー強国の建設の加速を提唱し、それをサイバーセキュリティ法に具体化するなど、データ関連規制の大幅な強化が図られており、**中国でサイバーセキュリティ業務に関連する事業者の取り巻く環境はより厳しくなることも想定**される。これまで以上に規制内容の正確な理解や、より慎重な経営判断が求められる局面もあり得るなど、規制の動向を注視しながらビジネスを行っていくことが求められる。

以上

別添 1

※機械翻訳

**全国人民代表大会常務委員会による『中華人民共和国サイバーセキュリティ法』改正に関する決定[20]（2025 年 10 月 28 日 第 14 回全国人民代表大会常務委員会第 18 回会議にて採択）**

第 14 回全国人民代表大会常務委員会第 18 回会議は、「中華人民共和国サイバーセキュリティ法」を下記の通り改正することを決定した：

一、新たに第三条を追加する：「サイバーセキュリティ業務は中国共産党の指導を堅持し、総体国家安全観を貫徹し、発展と安全を統一的に考慮し、サイバー強国の建設を推進する。」

二、第十八条を第十九条とし、第二項を削除する。

三、新たに一条を追加し、第二十条とする：「国は人工知能の基礎理論研究及びアルゴリズム等の重要技術開発を支援し、訓練データ資源、計算能力等のインフラ整備を推進し、人工知能倫理規範を整備し、リスク監視評価及び安全監督を強化し、人工知能の応用と健全な発展を促進する。国はサイバーセキュリティ管理方法の革新を支援し、人工知能等の新技術を活用して、サイバーセキュリティ保護水準の向上を図る。」

四、第四十条を第四十二条とし、新たに第二項を追加する：「ネットワークプロバイダが個人情報を処理する場合、本法及び『中華人民共和国民法典』、『中華人民共和国個人情報保護法』等の法律・行政法規の規定を遵守しなければならない。」

五、 第五十九条を第六十一条に改め、次のように修正する：「ネットワークプロバイダが本法第二十三条、第二十七条に規定するサイバーセキュリティ保護義務を履行しない場合、関係主管部門は是正を命じ、警告を与え、一万元以上五万元以下の罰金を科すことができる。是正を拒むか、サイバーセキュリティ危害等の結果を招いた場合、五万元以上五十万元以下の罰金を科し、直接責任を負う主管者及びその他の直接責任者に対し一万元以上十万元以下の罰金を科す。
「重要情報インフラ運営者が本法第三十五条、第三十六条、第三十八条、第四十条に規定するサイバーセキュリティ保護義務を履行しない場合、関係主管部門は是正を命じ、警告を与え、かつ五万元以上十万元以下の罰金を科すことができる。是正を拒むか、サイバーセキュリティを危害

[20] 全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定（全国人民代表大会サイト 2025 年 10 月 28 日）http://www.npc.gov.cn/npc/c2/c30834/202510/t20251028_449048.html

するなどの結果を招いた場合、十万元以上百万元以下の罰金を科し、直接責任を負う主管者及びその他の直接責任者に対し一万元以上十万元以下の罰金を科す。
「前二項の行為により、大量のデータ漏洩、重要情報インフラの部分的機能喪失等の重大なサイバーセキュリティ危害を招いた場合、関係主管部門は五十万元以上二百万元以下の罰金を科し、直接責任を負う主管者及びその他の直接責任者には五万元以上二十万元以下の罰金を科す。重要情報インフラの主要機能喪失等の特に深刻なサイバーセキュリティ危害の結果を生じた場合、200 万元以上 1000 万元以下の罰金を科し、直接責任を負う主管者及びその他の直接責任者に対し 20 万元以上 100 万元以下の罰金を科す。」

六、第六十条を第六十二条とし、新たに一項を追加し、第二項とする：「前項第一号及び第二号の行為により、本法第六十一条第三項に規定する結果を生じた場合、同項の規定に基づき処罰する。」

七、新たに一条を追加し、第六十三条とする：「本法第二十五条の規定に違反し、安全認証・安全検査を受けていない、安全認証不合格、安全検査基準不適合のネットワーク重要設備及びサイバーセキュリティ専用製品を販売又は提供した者は、関係主管部門により販売又は提供の停止を命じられ、警告を与えられ、違法所得を没収される。違法所得がない場合または違法所得が 10 万元未満である場合は、2 万元以上 10 万元以下の罰金を併科する。違法所得が 10 万元以上の場合は、違法所得の 1 倍以上 5 倍以下の罰金を併科する。情状が重い場合は、関連業務の停止、営業停止・改善命令、関連業務許可証の取消しまたは営業許可証の取消しを命ずることができる。法律・行政法規に別段の定めがある場合は、その規定による。」

八、第六十一条を第六十四条に改め、その中の「関係主管部門は関連業務の一時停止、営業停止による改善、ウェブサイトの閉鎖、関連業務許可証の取消しまたは営業許可証の取消しを命ずることができる」を「関係主管部門は関連業務の一時停止、営業停止による改善、ウェブサイトまたはアプリケーションの閉鎖、関連業務許可証の取消しまたは営業許可証の取消しを命ずることができる」に改める。

九、第六十二条を第六十五条に改め、次のように修正する：「本法第二十八条の規定に違反し、サイバーセキュリティ認証、検査、リスク評価等の活動を実施し、またはシステム脆弱性、コンピュータウイルス、サイバー攻撃、ネットワーク侵入等のサイバーセキュリティ情報を社会に発布した者は、関係主管部門により是正を命じられ、警告を与えられ、一万元以上十万元以下の罰金を科されることがある。是正を拒む場合または情状が重い場合には、10 万元以上 100 万元以下の罰金を科し、関連業務の一時停止、営業停止・改善、ウェブサイトまたはアプリケーションの閉鎖、関連業務許可証の取消しまたは営業許可証の取消しを命ずることができる。直接責任を負う主管者その他の直接責任者には 1 万元以上 10 万元以下の罰金を科す。

「前項の行為により、本法第 61 条第 3 項に規定する結果を生じた場合には、同項の規定に基づき処罰する。」

十、第六十五条を第六十七条に改め、次のとおり改正する。「重要情報インフラ運営者が本法第三十七条の規定に違反し、セキュリティ審査を受けていない、またはセキュリティ審査に合格していないネットワーク製品またはサービスを使用した場合、関係主管部門は期限を定めて是正、使用停止、国家安全への影響の除去を命じ、調達金額の 1 倍以上 10 倍以下の罰金を科し、直接責任を負う主管者その他の直接責任者には 1 万元以上 10 万元以下の罰金を科す。」

十一、 第六十八条及び第六十九条第一項を統合し、第六十九条として次のように改正する。「ネットワークプロバイダが本法第四十九条の規定に違反し、法律・行政法規で禁止されている情報の送信を停止せず、削除等の措置を講じず、関連記録を保存せず、関係主管部門に報告しなかった場合、または本法第五十二条の規定に違反し、関係部門の要求に従って法律・行政法規で禁止されている情報の送信を停止せず、削除等の措置を講じず、関連記録を保存しなかった場合、関係主管部門は是正を命じ、警告を与え、通報するとともに、5 万元以上 50 万元以下の罰金を科すことができる。是正を拒む場合または情状が重い場合には、50 万元以上 200 万元以下の罰金を科し、関連業務の一時停止、営業停止・改善、ウェブサイトまたはアプリケーションの閉鎖、関連業務許可証または営業許可証の取消しを命ずることができる。直接責任を負う主管者その他の直接責任者には 5 万元以上 20 万元以下の罰金を科す。
前項の行為により特に重大な影響または特に重大な結果を生じた場合、関係主管部門は 200 万元以上 1000 万元以下の罰金を科し、関連業務の停止、営業停止・改善、ウェブサイトまたはアプリケーションの閉鎖、関連業務許可証の取消しまたは営業許可証の取消しを命じ、直接責任を負う主管者その他の直接責任者に対し 20 万元以上 100 万元以下の罰金を科す。
「電子情報送信サービス提供者及びアプリケーションソフトウェアダウンロードサービス提供者が、本法第五十条第二項に規定する安全管理義務を履行しない場合、前二項の規定に基づき処罰する。」

十二、第六十四条、第六十六条及び第七十条を統合し、第七十一条として次のように改正する：「次の各号のいずれかの行為があった場合、関連法律・行政法規の規定に基づき処理・処罰する：
「(一) 本法第十三条第二項及びその他の法律・行政法規で禁止されている情報を公開または送信した場合；
「(二) 本法第二十四条第三項、第四十三条から第四十五条の規定に違反し、個人情報の権益を侵害した場合；
「(三) 本法第三十九条の規定に違反し、重要情報インフラ運営者が個人情報や重要データを国外に保存、または国外に提供した場合。

「本法第 46 条の規定に違反し、個人情報を窃取し、その他の不法な方法で取得し、不法に販売し、または不法に他人に提供した場合で、犯罪を構成しないときは、公安機関は関連する法律・行政法規の規定に基づき処罰する。」

十三、新たに一条を追加し、第七十三条とする：「本法の規定に違反したが、『中華人民共和国行政処罰法』に規定される情状酌量の余地がある、処罰を軽減する、または処罰しない事由に該当する場合は、その規定に基づき情状酌量の余地がある、処罰を軽減する、または処罰しない。」

十四、第七十五条を第七十七条とし、次のように改正する：「国外の機関、組織、個人が中華人民共和国のネットワーク安全に危害を加える活動に従事した場合、法に基づき法的責任を追及する。深刻な結果を招いた場合、国務院公安部門及び関係部門は、当該機関、組織、個人に対し、財産の凍結その他の必要な制裁措置を決定することができる。」

本決定は 2026 年 1 月 1 日から施行する。

『中華人民共和国サイバーセキュリティ法』は本決定に基づき相応の修正を加え、条文順序を調整した上で、改めて公布する。

別添 2

※CISTEC 仮訳

# 中華人民共和国サイバーセキュリティ法
## （2016 年 11 月 7 日第 12 期全国人民代表大会常務委員会第 24 回会議可決）[21]



### 第１章　総則

第１条

サイバーセキュリティを保障し、サイバースペースの主権と国家の安全、社会・公共利益を擁護し、公民・法人とその他の組織の合法権益を保護し、経済・社会情報化の健全な発展を促進するために、本法を制定する。

第２条

中華人民共和国の国内におけるネットワークの建設、運営、維持と使用、およびサイバーセキュリティの監督管理に、本法を適用する。

第３条

国家はサイバーセキュリティと情報化発展を同様に重んじることを堅持し、積極的利用、科学的発展、法による管理、安全確保の方針を遵守し、ネットワークインフラの建設と相互接続を推進し、ネットワークの技術革新と応用を奨励し、サイバーセキュリティの人材育成を支援し、健全なサイバーセキュリティ保障システムを構築し、サイバーセキュリティの保護能力を向上させる。

---

[21] http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm
http://news.xinhuanet.com/2016-11/07/c_1119867015.htm

第４条
国家はサイバーセキュリティ戦略を制定し、これを絶えず整備し、サイバーセキュリティを保障する基本的要求と主要目標を明らかにし、重点領域におけるサイバーセキュリティ政策、業務・任務と措置を打ち出す。

第５条
国家は措置を講じ、中華人民共和国の国内外で生じるサイバーセキュリティのリスクと脅威を監視、防御、処理し、最重要情報インフラが攻撃、侵入、妨害と破壊を受けないよう保護し、法に基づいてネットワーク違法犯罪活動を処罰し、サイバースペースの安全と秩序を維持する。

第６条
国家は誠実で信用を守り、健全で文明的な（モラルのある）ネットワーク行為を提唱し、社会主義の基本的価値観の普及を推進し、措置を講じて全社会のサイバーセキュリティ意識と水準を向上させ、全社会が共に参加してサイバーセキュリティを促進する良好な環境を構築する。

第７条
国家はサイバースペースのガバナンス、ネットワーク技術の研究開発と標準の制定、ネットワーク違法犯罪の取り締まりなどにおいて国際交流と協力を積極的に行い、平和で、安全で、開放的で、連携のとれたサイバースペースの構築を推進し、多国間の、民主的で、透明なネットワークガバナンスシステムを建設する。

第８条
国家のネットワーク情報部門は、サイバーセキュリティ業務と関連する監督管理業務の統括・調整を担当する。国務院の電信主管部門、公安部門とその他の関係機関は本法と関連する法律・行政法規の規定に基づいて、各自の職責の範囲内でサイバーセキュリティの保護と監督管理業務を担当する。
県級以上の地方人民政府関連部門のサイバーセキュリティ保護と監督管理の職責は、国家の関連規定に基づいて確定する。

第９条
通信事業者が行う経営とサービス活動は、法律・行政法規を遵守し、社会道徳を尊重し、商業倫理、誠実信用を遵守し、サイバーセキュリティの保護義務を履行し、政府と社会の監督を受け、社会責任を負わなければならない。

第１０条
ネットワークの建設・運営あるいはネットワークを通じてサービスを提供するには、法律・行政法規の規定と国家標準の強制的要求事項に基づいて、技術的措置とその他の必要な措置を講

じ、ネットワークの安全、安定した運用を保障し、サイバーセキュリティ事件に効果的に対応し、ネットワークの違法犯罪活動を防止し、ネットワークデータの完全性、秘密保守性と可用性を維持しなければならない。

第１１条

ネットワーク関連産業組織は定款に基づいて、産業の自律性を強化し、サイバーセキュリティ行動規範を制定し、会員を指導してサイバーセキュリティの保護を強化し、サイバーセキュリティ保護の水準を向上させ、産業の健全な発展を促進する。

第１２条

国家は公民、法人とその他組織が法に基づいてネットワークを使用する権利を保護し、ネットワーク接続の普及を促進し、ネットワークサービスの水準を向上させ、社会に安全で、便利なネットワークサービスを提供し、ネットワーク情報の法に基づく秩序をもった自由な流動を保障する。

いかなる個人と組織もネットワークを使用するには、憲法・法律を遵守し、公共の秩序を遵守し、社会道徳を尊重し、サイバーセキュリティに危害を加えてはならず、ネットワークを利用して国家の安全、栄誉と利益に危害を加える、国家・政権の転覆、社会主義制度の打倒を扇動する、国家の分裂、国家統一の破壊を扇動する、テロリズムと過激主義を宣伝する、民族憎悪、民族差別を宣伝する、暴力、猥褻・性的な情報を伝播する、虚偽情報をねつ造・伝播させて経済秩序と社会秩序をかく乱させる、および他人の名誉、プライバシー、知的財産権とその他の合法的権益を侵害するなどの活動に従事してはならない。

第１３条

国家は未成年の健全な成長に資するネットワーク製品とサービスの研究開発を支援し、法に基づいてネットワークを利用して未成年の心身の健康に危害を加える活動を処罰し、未成年のために安全で、健全なネットワーク環境を提供する。

第１４条

いかなる個人と組織もサイバーセキュリティに危害を加える行為に対して、ネットワーク情報、電信、公安などの部門に通報する権利を持つ。通報を受けた部門は速やかに法に基づいて処理を行わなければならない。；当該部門の職責に属さないものは、速やかに処理権限をもつ部門に引き渡さなければならない。

関連部門は通報者に関わる情報に対して秘密を保守し、通報者の合法権益を保護しなければならない。

第２章　サイバーセキュリティの支援と促進

第１５条

国家はサイバーセキュリティの標準体系を建設・整備する。国務院の標準化の行政主管部門と国務院のその他の関係部門は各自の職責に基づいて、サイバーセキュリティの管理とネットワーク製品・サービスと運用の安全にかんする国家標準、業界標準を制定し、適時に修正する。

国家は企業、研究機構、高等教育機関、ネットワーク関連産業組織がサイバーセキュリティの国家標準、業界標準の制定に参加することを支援する。

第１６条

国務院と省・自治区・直轄市の人民政府は統一的に計画し、投資を拡大し、重点サイバーセキュリティ技術産業とプロジェクトを支援し、サイバーセキュリティ技術の研究開発と応用を支援し、安全で信頼できるネットワーク製品とサービスを普及させ、ネットワーク技術の知的財産権を保護し、企業・研究機構と高等教育機関などが国家のサイバーセキュリティ技術革新プロジェクトに参加することを支援しなければならない。

第１７条

国家はサイバーセキュリティの社会化されたサービスシステム建設を推進し、関連企業・機構が行うネットワーク安全（サイバーセキュリティ）認証、検査・試験とリスク評価などの安全サービスを奨励する。

第１８条

国家はネットワークデータの安全保護と利用技術の開発を奨励し、公共デーのタ資源開放を促進し、技術革新と経済社会の発展を推進する。

国家はサイバーセキュリティの管理方式を革新し、ネットワークの新技術を駆使し、サイバーセキュリティの保護水準を向上させることを支援する。

第１９条

各級人民政府とその関連部門は、経常的なサイバーセキュリティの宣伝教育を行い、また関連団体がサイバーセキュリティ宣伝教育活動をしっかり行うよう指導・督促しなければならない。

マスメディアは狙いをはっきりさせて社会にむけてサイバーセキュリティの宣伝教育を行わなければならない。

第２０条

国家は企業と高等教育機関、職業学校などの教育研修機関がサイバーセキュリティに関わる教育と研修を行うことを支援し、さまざまな方式を講じてサイバーセキュリティの人材を育成し、サイバーセキュリティの人材交流を促進する。

## 第３章　ネットワーク運用のセキュリティ

### 第１節　一般規定

第２１条　国家はサイバーセキュリティ等級保護制度を実行する。通信事業者はセイバーセキュリティ等級保護制度の要求に基づいて、以下の安全保護義務を履行し、ネットワークが妨害、破壊あるいは無許可のアクセスを受けないように保障し、ネットワークデータの漏えいあるいは窃取、改ざんを防止しなければならない。

（１）内部安全管理制度と操作規程を制定し、サイバーセキュリティの責任者を定め、サイバーセキュリティの保護責任を着実に果たす。

（２）コンピュータウイルスとサイバー攻撃、ネットワーク侵入などのサイバーセキュリティに危害を加える行為を防止する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事件を監視・記録する技術的措置を講じ、また、規定に基づいて関連するネットワークログの保存を六か月より短くしてはならない。

（４）データの分類、重要データのバックアップと暗号化などの措置を講じる。

（５）法律・行政法規で規定したその他の義務。

第２２条

ネットワーク製品、サービスは関連する国家標準の強制的要求に符合していなければならない。ネットワーク製品、サービスの提供者は悪意のあるソフトウェアを設置してはならない。；そのネットワーク製品、サービスにセキュリティ上の欠陥、脆弱性などのリスクを発見したならば、速やかに救済措置を講じ、規定に基づいて速やかにユーザーに告知し、関連主管部門に報告しなければならない。

ネットワーク製品、サービスの提供者はその製品、サービスのセキュリティメンテナンスを持続的に提供しなければならない。；規定あるいは当事者と取り決めた期間内において、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。

ネットワーク製品、サービスでユーザー情報を収集する機能を備えているものは、提供者がユーザーにそのことを明示し同意を得なければならない。ユーザーの個人情報に関わるものは、本法と関連法律、行政法規の個人情報保護にかんする規定を遵守しなければならない。

第２３条

ネットワークの最重要設備とサイバーセキュリティの専用製品は、関連する国家標準の強制的要求に基づいて、資格を備えた機構の安全認証に合格する、あるいはセキュリティ検査試験の要求事項に符合したのちに、販売あるいは提供することができる。国家のネットワーク情報部門が国務院の関連部門と共同でネットワーク最重要設備とサイバーセキュリティ専用製品目録を制定・公布し、安全認証と安全検査・試験の結果の相互承認を推進し、認証と検査・試験の重複しないようにする。

第２４条

通信事業者がユーザーのネットワーク接続、ドメイン登録サービスの手続き、固定電話、携帯電話などの接続手続き、あるいはユーザーに情報発布、インスタントメッセージなどのサービスを提供するには、ユーザーとの契約、あるいは提供するサービスの確認時に、ユーザーに真実の身分情報を提供するよう求めなければならない。ユーザーが真実の身分情報を提供しなければ、通信事業者は関連するサービスを提供してはならない。

国家はネットワークにおける信頼できるアイデンティティのための戦略を実施し、安全で、便利な電子身分認証技術の研究開発を支援し、さまざまな電子身分認証間の相互認証を推進する。

【参考】：なお、アメリカの国土安全保障省は 2010 年 6 月に「National Strategy for Trusted Identities in Cyberspace：NSTIC」（サイバースペースにおける信頼できるアイデンティティのための国家戦略）を発表した[22]。

第２５条

通信事業者はサイバーセキュリティ事件の緊急対策案を制定し、システムの脆弱性、コンピュータウイルス、サイバー攻撃、ネットワーク侵入などのセキュリティリスクを速やかに処理しなければならない。；サイバーセキュリティに危害を加える事件の発生時には、即座に緊急対策案を始動し、相応の救済措置を講じ、規定に基づいて関連主管部門に報告しなければならない。

第２６条

ネットワークの安全認証、検査・試験、リスク評価などの活動を行い、社会に向けてシステムの脆弱性、コンピュータウイルス、サイバー攻撃、ネットワーク侵入などのサイバーセキュリティの情報を公表するには、国家の関連規定を遵守しなければならない。

第２７条

いかなる個人と組織も不法に他人のネットワークに侵入する、他人のネットワークの正常な機能を妨害する、ネットワークデータを窃取するなどのサイバーセキュリティに危害を加える活動に従事してはならない。；ネットワーク侵入、ネットワークの正常な機能と防御措置の妨害、ネットワークデータの窃取などのサイバーセキュリティに危害を加える活動に従事するための専用のプログラムやツールを提供してはならない。；他人がサイバーセキュリティに危害を加える活動に従事していることを明らかに知ったさいには、技術支援、宣伝・普及、支払清算などの援助を提供してはならない。

第２８条

通信事業者は公安機関・国家安全機関の法に基づく国家安全と犯罪捜査の活動に技術支援と協力を提供しなければならない。

---

[22] http://www.dhs.gov/xlibrary/assets/ns_tic.pdf

第２９条

国家は通信事業者の間でサイバーセキュリティの情報収集、分析、通報と応急処置などにおける協力を行い、通信事業者の安全保障能力を向上させることを支援する。

関連する産業組織は、健全な当該産業のサイバーセキュリティ保護規定と協力の枠組みを構築し、サイバーセキュリティのリスクに対する分析評価を強化し、定期的に会員に向けてリスクにかんする注意を促し、会員のサイバーセキュリティのリスク対応を支援・協力する。

第３０条

国家のネットワーク情報部門と関連部門がサイバーセキュリティ保護の職責履行の中で取得した情報は、サイバーセキュリティを維持管理する必要で使用するのみとし、その他の用途に用いてはならない。

第２節　最重要情報インフラ運用の安全

第３１条

国家は、公共通信と情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政務などの重要産業と分野、およびひとたび破壊、機能喪失、あるいはデータ漏えいなどに遭ったならば、国家安全、国の経済と人民の生活、公共の利益に深刻な危害が加えられる恐れのある最重要情報インフラに対して、サイバーセキュリティ等級保護制度を基礎として、重点保護を実施する。最重要情報インフラ施設の具体的な範囲とセキュリティ保護方弁法は国務院が制定する。

国家は最重要情報インフラ以外の通信事業者が自ら志願して重要情報インフラの保護体系に参加することを奨励する。

第３２条

国務院の規定する職責分業に基づいて、最重要情報インフラのセキュリティ保護業務を担当する部門はそれぞれ当該産業、当該領域の最重要情報インフラの安全計画を作成して実行し、最重要情報インフラ運用のセキュリティ保護業務を指導・監督する。

第３３条

最重要情報インフラの建設には、それが業務の安定した、持続的な運営をサポートするという性能を備えていることを確実に保証し、セキュリティの技術的措置が計画と歩調をそろえ、建設と歩調をそろえ、使用と歩調をそろえていることを保証しなければならない。

第３４条　本法第２１条の規定を除き、最重要情報インフラの運営者はさらに以下のセキュリティ保護義務を履行しなければならない。：

（１）専門のセキュリティ管理機構とセキュリティ管理の責任者を設け、当該責任者と重要な職位にある人員に対してセキュリティにかんするバックグラウンドチェックを行う。

（２）定期的に従業員に対してサイバーセキュリティ教育、技術研修と技能試験を行う。
（３）重要システムとデータベースに対して災害対策のためのバックアップを行う。
（４）サイバーセキュリティ事件の緊急対応策を制定し、定期的に訓練を行う。
（５）法律・行政法規で定めたその他の義務。

第３５条
最重要情報インフラの運営者がネットワーク製品とサービスを調達するさいに、国家の安全に影響を及ぼすであろうものには、国家のネットワーク情報部門が国務院の関連部門と合同で行う国家安全審査に合格しければならない。

第３６条
最重要情報インフラの運営者がネットワーク製品とサービスを調達するには、規定に基づいて提供者とセキュリティにかんする秘密保守協議を交わし、セキュリティと秘密保守義務と責任を明確にしなければならない。

第３７条
最重要情報インフラの運営者が中華人民共和国国内の事業のなかで収集・作成した個人情報と重要データは国内で保存しなければならない。業務の必要により、確かに国外に提供しなければならないものは、国家のネットワーク情報部門が国務院の関連部門と共同で制定した規則に基づいて安全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ものは、その規定に基づく。

第３８条
最重要情報インフラの運営者は自らあるいはサイバーセキュリティサービス機構に委託してそのネットワークの安全性と存在するであろうリスクに対して毎年少なくとも一回の検査・評価を行い、検査・評価の状況と改善措置を関連する最重要情報インフラのセキュリティ保護業務を担当する部門に申告しなければならない。
第３９条　国家のネットワーク情報部門は、関連部門を統括・調整して、最重要情報インフラのセキュリティ保護に対して以下の措置を講じなければならない。
（１）最重要情報インフラのセキュリティリスクに対してサンプリング調査を行い、改善措置を提出し、必要なときにはサイバーセキュリティサービス機構に委託してネットワークに存在するセキュリティリスクに対して検査・評価を行うことができる。
（２）定期的に最重要情報インフラの運営者にたいしてサイバーセキュリティの緊急対応訓練を行い、サイバーセキュリティ事件に対応する水準と共同協力能力を向上させる。
（３）関連部門、最重要情報インフラの運営者および関連研究機構、サイバーセキュリティサービス機構などの間のサイバーセキュリティの情報共有を促進する。

（４）サイバーセキュリティ安全事件の緊急対応処置とネットワーク機能の復旧などに対して、技術支援と協力を提供する。

## 第４章　ネットワーク情報のセキュリティ

### 第４０条

通信事業者はその収集したユーザー情報に対して厳格に秘密を保守し、そのうえ健全なユーザー情報の保護制度を構築しなければならない。

### 第４１条

通信事業者が個人情報を収集・使用するさいには、合法、正当、必要という原則を遵守し、収集・使用規則を公開し、情報を収集・使用する目的・方式と範囲を明示し、被収集者の同意を得なければならない。

通信事業者は提供するサービスと関係のない個人情報を収集してはならず、法律・行政法規の規定と双方の個人情報収集・使用にかんする取り決めに違反してはならず、また、法律・行政法規の規定とユーザーとの取り決めに基づいて、保存した個人情報を処理しなければならない。

### 第４２条

通信事業者は収集した個人情報を漏えい、改ざん、毀損してはならない。；被収集者の同意を得ずに、他人に個人情報を提供してはならない。ただし、特定の個人を識別することができず、かつ復元できないよう処理を施したものは除く。

通信事業者は技術的措置とその他の必要な措置を講じ、収集した個人情報のセキュリティを確実に保証し、情報の漏えい、毀損、紛失を防止しなければならない。個人情報の漏えい、毀損、紛失などの状況が発生、あるいは発生する可能性があるさいには、速やかに救済措置を講じ、規定に基づいて速やかにユーザーに告知し、そのうえ関連主管部門に報告しなければならない。

### 第４３条

個人が、通信事業者が法律、行政法規の規定、あるいは双方の取り決めに違反してその個人情報を収集・使用したことを発見したならば、通信事業者にその個人情報を削除するよう要求する権利を有する。；通信事業者が収集・保存している個人情報に誤りのあることを発見したならば、通信事業者に対して訂正を要求する権利を有する。通信事業者は措置を講じて削除あるいは訂正しなければならない。

### 第４４条

いかなる個人と組織も個人情報を窃取する、あるいはその他の不法な方式で取得してはならず、個人情報を不法に販売する、あるいは不法に他人に提供してはならない。

第４５条

法に基づいてサイバーセキュリティの監督管理の職責を負う部門とその業務従事者は、職責を履行するなかで知った個人情報、プライバシーと商業秘密に対して厳格に秘密を保守しなければならず、漏えい、販売あるいは不法に他人に提供してはならない。

第４６条

いかなる個人と組織もその使用するネットワークの行為に対して責任を負い、詐欺、犯罪方法を伝授する、禁令に違反する物品、規制している物品を製作あるいは販売するなどの違法犯罪活動を実施するのに用いるウェブサイト、通信クラスターを設立してはならず、ネットワークを利用して詐欺、禁令に違反する物品、規制している物品を製作あるいは販売する、およびその他の違法犯罪活動にかかわる情報を公表してはならない。

第47条

通信事業者はユーザーが発布した情報に対する管理を強化し、法律・行政法規で公表あるいは発信を禁止する情報を発見したならば、速やかに当該情報の発信を停止し、削除などの処理・措置を講じ、情報の拡散を防止し、関連する記録を保存し、関連主管部門に報告しなければならない。

第４８条

いかなる個人・組織であろうとも、発信する電子情報、提供するアプリケーションソフトウェアに悪意のあるソフトウェアを組み込んではならず、法律・行政法規で発布あるいは発信を禁止する情報を含めてはならない。

電子情報の送信サービス提供者とアプリケーションソフトウェアのダウンロードサービス提供者は、セキュリティ管理義務を履行しなければならず、ユーザーに前項で規定した行為のあることを知ったならば、サービスの提供を停止し、削除などの処理・措置を講じ、関連する記録を保存し、関連主管部門に報告しなければならない。

第４９条

通信事業者はネットワークの情報セキュリティの投書・通報制度を構築し、投書・通報方法などの情報を公表し、ネットワークの情報セキュリティにかんする投書と通報を速やかに受理し処理しなければならない。

通信事業者はネットワーク情報部門が法に従って実施する監督検査に、協力しなければならない。

第５０条

国家のネットワーク情報部門と関連部門が法に従って履行するネットワークの情報セキュリティ監督管理の職責において、法律・行政法規で公表あるいは発信を禁止する情報を発見したなら

ば、通信事業者に発信を停止するよう求め、削除などの処理・措置を講じ、関連する記録を保存しなければならない。；中華人民共和国の国外に由来する上述の情報に対しては、関連機関に通知して技術的措置とその他の必要な措置を講じて伝播を阻止しなければならない。

## 第５章　監視・早期警戒と緊急対応処置

### 第５１条

国家はサイバーセキュリティの監視・早期警戒と情報の通報制度を構築する。国家のネットワーク通信部門は関連部門を統括・調整してサイバーセキュリティの情報収集、分析と通報活動を強化し、規定に基づいてサイバーセキュリティの監視・早期警戒情報を統括して発布しなければならない。

### 第５２条

最重要情報インフラの安全保護業務を担当する部門は、当該産業、当該領域におけるサイバーセキュリティの監視・早期警戒と情報の通報制度を構築し、規定に基づいてサイバーセキュリティの監視・早期警戒情報を報告しなければならない。

### 第５３条

国家のネットワーク情報部門は、関連部門と協調して健全なサイバーセキュリティのリスク評価と緊急対応業務の枠組みを構築し、サイバーセキュリティ事件の緊急対応策を制定し、定期的に訓練を行う。

重要情報インフラのセキュリティ保護業務を担当する部門は、当該産業、当該領域におけるサイバーセキュリティ緊急対応策を制定し、定期的に訓練を行わなければならない。

サイバーセキュリティ事件の緊急対応策は事件発生後の被害の程度、影響範囲などの要素に応じてサイバーセキュリティ事件に対する等級区分を行い、相応の緊急対応処理・措置を規定しなければならない。

### 第５４条

サイバーセキュリティ事件が発生するリスクが増大したさいに、省級以上の人民政府関連部門は規定の権限と手順に基づいて、サイバーセキュリティのリスクの特徴と起こりうる被害に基づいて、以下の措置を講じなければならない。：

（１）関連部門、機構と人員に速やかに関連情報を収集し報告するよう要求し、サイバーセキュリティのリスクの監視を強化する。

（２）関連部門、機構と専門人員を組織して、サイバーセキュリティのリスク情報に対して分析・評価を行い、事件の発生する可能性、影響する範囲と被害の程度を予測する。

（３）社会に向けてサイバーセキュリティのリスクの早期警戒を発布し、被害を回避・軽減する措置を公表する。

第５５条

サイバーセキュリティ事件が発生したら、速やかにサイバーセキュリティ緊急対応策を始動し、サイバーセキュリティ事件に対して調査と評価を行い、通信事業者に技術的措置とその他の必要な措置を講じるよう要求し、セキュリティの潜在的危険を除去し、被害の拡大を防止し、そのうえ速やかに社会にむけて公衆に関係のある警告情報を公表しなければならない。

第５６条

省級以上の人民政府関連部門はサイバーセキュリティの監督管理の職責において、ネットワークに比較的大きなセキュリティリスクが存在することを発見した、あるいは安全事件が発生したならば、規定の権限と手順に基づいて、当該ネットワークの運営者の法定代表人あるいはその主要責任者に対して事情聴取を行うことができる。通信事業者は要求に基づいて措置を講じ、改善を行い、潜在的危険を除去しなければならない。

第５７条

サイバーセキュリティ事件によって、突発事件あるいは安全生産事故が発生したならば、《中華人民共和国突発事件応対法》、《中華人民共和国安全生産法》などの関連法律・行政法規の規定に基づいて処置を行わなければならない。

第５８条

国家の安全と社会の公共秩序を擁護するために、重大な社会安全の突発事件を処理する必要があるさいには、国務院の決定あるいは批准を経て、特定地域においてネットワーク通信に対する制限などの臨時措置を講じることができる。

## 第６章　法律責任

第５９条

通信事業者が本法第２１条、第２５条に規定したサイバーセキュリティの保護義務を履行しなかったならば、関連主管部門が是正を命じ、警告を与える。；是正を拒否する、あるいはサイバーセキュリティに危害を加えるなどの結果をもたらしたならば、１万人民元以上１０万人民元以下の罰金を科し、直接責任を負う主管者に対しては５０００人民元以上５万人民元以下の罰金を科す。

最重要情報インフラの運営者が本法第３３条、第３４条、第３６条、第３８条に規定したサイバーセキュリティの保護義務を履行しなかったならば、関連主管部門が是正を命じ、警告を与える。；是正を拒否する、あるいはサイバーセキュリティに危害を加えるなどの結果をもたらしたならば、１０万人民元以上１００万人民元以下の罰金を科し、直接責任を負う主管者に対しては１万人民元以上１０万人民元以下の罰金を科す。

第６０条

本法第２２条第１項、第２項と第４８条第１項の規定に違反し、以下の行為の一つがあったならば、関連主管部門が是正を命じ、警告を与える。；是正を拒否する、あるいはサイバーセキュリティに危害を加えるなどの結果をもたらしたならば、５万人民元以上５０万人民元以下の罰金を科し、直接責任を負う主管者に対しては１万人民元以上１０万人民元以下の罰金を科す。

（１）悪意のあるプログラムを組み込んだ；

（２）製品、サービスに存在する安全上の欠陥、脆弱性などのリスクに対して、速やかに救済措置を講じず、あるいは規定に従わずに即座にユーザーに告知してない、主管部門にも報告していない；

（３）製品、サービスのセキュリティのメンテナンスを無断で終了する。

第６１条

通信事業者が本法第２４条第１項の規定に違反し、ユーザーに真実の身分情報の提供を要求していない、あるいは真実の身分情報を提供していないユーザーに対して関連するサービスを提供したならば、関連主管部門が是正を命じる。；是正を拒否する、あるいは事案の深刻なものは、５万人民元以上５０万人民元以下の罰金を科し、また関連主管部門が関連業務の一時停止、業務停止・業務の再構築、ウェブサイトの閉鎖、関連業務の許可証の取り上げ、あるいは営業許可証の取り上げを命じることができ、直接責任を負う主管者とその他の直接責任を負う人員に対しては、１万人民元以上１０万人民元以下の罰金を科す。

第６２条

本法第２６条の規定に違反し、ネットワークの安全認証（サイバーセキュリティ認証）・検査・リスク評価などの活動を行う、あるいは社会に向けてシステムの脆弱性、コンピュータウイルス、サイバー攻撃、ネットワーク侵入などのサイバーセキュリティ情報を発布したならば、是正を命じ、警告を与える。；是正を拒否するあるいは事案が深刻なものは、１万人民元以上１０万人民元以下の罰金を科し、また関連主管部門が関連業務の一時停止、業務停止・業務の再構築、ウェブサイトの閉鎖、関連業務の許可証の取り上げ、あるいは営業許可証の取り上げを命じることができ、直接責任を負う主管者とその他の直接責任を負う人員に対しては、５０００人民元以上５万人民元以下の罰金を科す。

第６３条

本法第２７条の規定に違反し、サイバーセキュリティに危害を加える活動に従事する、あるいはサイバーセキュリティに危害を加える活動に従事するための専用のプログラム・ツールを提供する、あるいは他人が従事するサイバーセキュリティに危害を加える活動に技術支援、広告・普及、支払・決済などの援助を提供したならば、まだ犯罪を構成していないものは、公安機関が違法所得を没収し、５日以下の勾留に処し、５万人民元以上５０万人民元以下の罰金を併科すこと

ができる；事案の比較的深刻なものは、５日以上１５日以下の勾留に処し、１０万人民元以上１００万人民元以下の罰金を併科することができる。

団体で前項に規定した行為があれば、公安機関が違法所得を没収し、１０万人民元以上１００万人民元以下の罰金を科し、直接責任を負う主管者とその他の直接責任を負う人員は前項の規定に従って処罰する。

本法第２７条の規定に違反し、保安・監督処分を受けた人員は、五年以内にサイバーセキュリティの管理と通信事業の最も重要な職位の業務に従事することはできない。；刑事処罰を受けた人員は、終身、サイバーセキュリティの管理と通信事業の最も重要な職位の業務に従事することはできない。

第６４条

通信事業者、ネットワーク製品あるいはサービスの提供者が本法第２２条第３項、第４１条から第４２条の規定に違反し、個人情報の法に従って保護を受ける権利を侵害したならば、関連主管部門が是正を命じ、事案に基づいて、警告、違法所得の没収、違法所得の１倍以上１０倍以下の罰金を科す、あるいは併科し、違法所得のないものは、１００万人民元以下の罰金を科し、直接責任を負う主管者とその他の直接責任を負う人員に対しては、１万人民元以上１０万人民元以下の罰金を科す。；事案の深刻なものは、関連業務の一時停止、業務停止・業務の再構築、ウェブサイトの閉鎖、関連業務の許可証取り上げあるいは営業許可証の取り上げを命じることもできる。

本法第４４条の規定に違反し、個人情報を窃取する、あるいはその他の方式で不法に獲得する、不法に販売するあるいは不法に他人に提供したならば、また犯罪を構成していないものは、公安機関が違法所得を没収し、そのうえ違法所得の１倍以上１０倍以下の罰金を科し、違法所得のないものは１００万人民元以下の罰金を科す。

第６５条

最重要情報インフラの運営者が本法第３５条の規定に違反し、安全審査を受けていない、あるいは安全審査にまだ合格していないネットワーク製品あるいはサービスを使用したならば、関連主管部門は使用停止を命じ、調達金額の１倍以上１０倍以下の罰金を科す。；直接責任を負う主管者とその他の直接責任を負う人員に対しては１万人民元以上１０万人民元以下の罰金を科す。

第６６条

最重要情報インフラの運営者が本法第３７条の規定に違反し、国外でネットワークデータを保存する、あるいは国外にネットワークデータを提供したならば、関連主管部門が是正を命じ、警告を与え、違法所得を没収し、５万人民元以上５０万人民元以下の罰金を科し、また関連業務の一時停止、業務停止・業務の再構築、ウェブサイトの閉鎖、関連業務の許可証の取り上げあるいは営業許可証の取り上げを命じることができる。；直接責任を負う主管者とその他の直接責任を負う人員に対しては、１万人民元以上１０万人民元以下の罰金を科す。

第６７条

本法第４６条の規定に違反し、違法な犯罪活動実施に用いるウェブサイト、通信クラスターを設立する、あるいはネットワークを利用して違法犯罪活動実施にかかわる情報を発布したならば、また犯罪を構成していないものは、公安機関は５日以下の勾留に処し、５万人民元以上５０万人民元以下の罰金を科すこともできる。違法犯罪活動実施に用いるウェブサイト、通信クラスターを閉鎖する。

団体で前項の行為のあるものは、公安機関が１０万人民元以上５０万人民元以下の罰金を科し、また直接責任を負う主管者とその他の直接責任を負う人員に対して前項の規定に基づいて処罰することができる。

第６８条

通信事業者が本法第４７条の規定に違反し、法律・行政法規で発布あるいは伝送を禁止する情報がいまだ伝送を停止しておらず、削除などの処置・措置を講じておらず、関連する記録を保存していないものに対しては、関連主管部門が是正を命じ、警告を与え、違法所得を没収する。；是正を拒否する、あるいは事案が深刻なものは、１０万人民元以上５０万人民元以下の罰金を科し、また関連業務の一時停止、業務停止・業務の再構築、ウェブサイトの閉鎖、関連業務の許可証取り上げあるいは営業許可証の取り上げを命じ、直接責任を負う主管者とその他の直接責任を負う人員に対して、１万人民元以上１０万人民元以下の罰金を科すことができる。

電子情報送信サービスの提供者、アプリケーションソフトウェアのダウンロードサービス提供者が、本法第４８条第２項に規定した安全（セキュリティ）管理義務を履行していなければ、前項の規定にしたがって処罰する。

第６９条

通信事業者が本法の規定に違反し、以下の行為の一つがあったならば、関連主管部門が是正を命じる。；是正を拒否する、あるいは事案が深刻なものは、５万人民元以上５０万人民元以下の罰金を科し、直接責任を負う主管者とその他の直接責任を負う人員は、１万人民元以上１０万人民元以下の罰金を科す。：

（１）関連部門の要求に基づいて法律・行政法規で発布あるいは伝送を禁止する情報に対して、伝送停止・削除などの処置・措置を講じていない；

（２）関連部門が法に基づいて実施する監督検査を拒否、妨害する；

（３）公安機関・国家安全機関への技術支援と協力の提供を拒否する。

第７０条

本法第１２条第２項とその他の法律・行政法規で発布あるいは伝送を禁止する情報を発布・伝送したならば、関連する法律・行政法規の規定に基づいて処罰する。

第７１条

本法で規定した違法行為があったならば、関連法律・行政法規の規定に基づいて信用記録に記載し、これを公示する。

第７２条

国家機関の政務ネットワークの運営者が本法で規定したネットワーク安全（サイバーセキュリティ）保護義務を履行しなかったならば、その上級機関あるいは関連機関が是正を命じる。；直接責任を負う主管者とその他の直接責任を負う人員に対しては法に従って処分する。

第７３条

ネットワーク情報部門と関連部門が本法第３０条の規定に違反し、ネットワーク安全（サイバーセキュリティ）保護の職責のなかで獲得した情報をその他の用途に用いたならば、直接責任を負う主管者とその他の直接責任を負う人員を法に基づいて処分する。

ネットワーク情報部門と関連部門の業務人員が、職務をおろそかにする、職権を濫用する、私情にとらわれて不正を働いたならば、まだ犯罪を構成していないものは、法に基づいて処分する。

第７４条

本法の規定に違反し、他人に損害をもたらしたならば、法に基づいて民事責任を負う。

本法の規定に違反し、保安・監督行為違反を構成するものは、法に基づいて保安・監督処罰を与える。；犯罪を構成するものは、法に基づいて刑事責任を追及する。

第７５条

国外の機構・組織・個人が攻撃・侵入・妨害・破壊などの中華人民共和国の最重要情報基礎施設（インフラ）に危害を加える活動に従事し、深刻な悪影響をもたらせたならば、法に基づいて法律責任を追及する。国務院の公安部門と関連部門は当該機構・組織・個人に対して財産を凍結する、あるいはその他の必要な制裁措置をとることを決定することもできる。

第７章　附則

第７６条　本法における以下の用語の意味：

（１）網絡（ネットワーク）とは、コンピュータとその他の情報端末および関連設備から構成される一定の規則とプログラムに基づいて情報に対して収集・保存・伝送・交換・処理を行うシステムを指す。

（２）網絡安全（サイバーセキュリティ）とは、必要な措置を講じて、ネットワークに対する攻撃・侵入・妨害・破壊と不正使用および不測の事故を防止し、ネットワークを安定的に信頼できる運用状態にあらしめ、またネットワークデータの完全性、機密性、可用性といった能力を保障することを指す。

（3）通信事業者とは、ネットワークの所有者・管理者とネットワークサービスの提供者（ネットワークサービスプロバイダ）を指す。

（4）ネットワークデータとは、ネットワークを通じて収集・保存・伝送・処理・生成した各種電子データを指す。

（5）個人情報とは、電子あるいはその他の方式で記録した単独で、あるいはその他の情報と結び付けて個人の身分を識別することのできる各種情報を指し、これには自然人の姓名、出生期日、身分証番号、個人生体認証情報、住所、電話番号などが含まれる。

第７７条

国家秘密にかかわる情報を保存・処理するネットワークの運用のセキュリティ保護は、本法を遵守しなければならないほかに、さらに秘密保守の法律、行政法規の規定を遵守しなければならない。

第７８条

軍事ネットワークのセキュリティ保護は、中央軍事委員会が別途規定する。

第７９条

本法は２０１７年6月1日より施行する。