最終更新日：2026 年 3 月 12 日

中華人民共和国サイバーセキュリティ法 （仮訳）

（2016 年 11 月 7 日第十二期全国人民代表大会常務委員会第二十四回会議において採択、2025 年 10 月 28 日第十四期全国人民代表大会常務委員会第十八回会議「『中華人民共和国サイバーセキュリティ法』の改正に関する決定」に基づき改正。）

目　録

第一章　総　則

第一条　ネットワークの安全を保障し、サイバー空間の主権と国家安全および社会公共利益を維持し、公民、法人、その他組織の合法的権益を保護し、経済社会の情報化の健全な発展を促進するため、本法を制定する。
第二条　中華人民共和国国内におけるネットワークの構築、運営、メンテナンス、使用、およびサイバーセキュリティの監督管理において、本法を適用する。
第三条　サイバーセキュリティ業務において中国共産党の指導を堅持し、総体的国家安全観を貫徹し、発展と安全を統一的に計画し、サイバー強国の構築を推進する。
第四条　国はサイバーセキュリティと情報化の発展の重要性を並行して堅持し、積極的利用、科学的発展、法に基づく管理、安全確保の方針に従い、ネットワークインフラストラクチャの構築およびコネクティビティを推進し、ネットワーク技術のイノベーションと応用を奨励し、サイバーセキュリティ人材の育成を支持し、健全なサイバーセキュリティ保障体系を構築し、サイバーセキュリティ保護能力を高める。
第五条　国はサイバーセキュリティ戦略を制定すると共に絶えず改善し、ネットワークの安全を保障する基本的要求と主な目標を明確にし、重点分野であるサイバーセキュリティの政策、業務任務および措置を提出する。
第六条　国は措置を講じ、中華人民共和国国内外に由来するサイバーセキュリティリスクと脅威をモニタリング、防御、処置し、重要情報インフラストラクチャを攻撃、侵入、妨害、破壊から保護し、法に従ってサイバー犯罪活動を処罰し、サイバー空間の安全と秩序を維持する。
第七条　国は、信義則による健全で教養あるネットワーク行為を提唱し、社会主義の核心的価値観の伝播を推進し、社会全体のサイバーセキュリティ意識とレベルを高める措置を講じ、社会全体がサイバーセキュリティの促進に共に参与する良好な環境を形成する。
第八条　国はサイバー空間ガバナンス、サイバー技術の研究開発と規格制定、サイバー犯罪の取締りなどの面において国際交流と協力を積極的に展開し、平和で安全、かつ開放的、協力的なサイバー空間の構築を推進し、多国間での、民主的で透明性のあるサイバーガバナンス体系を構築する。
第九条　国家インターネット情報部門は、サイバーセキュリティ業務および関連監督管理業務の統一的な計画・調整に責任を負う。国務院の電信主管部門、公安部門およびその他関係機関

は、本法および関連法律、行政法規の規定に基づき、各自の職責範囲内でサイバーセキュリティ保護および監督管理業務に責任を負う。

県級以上の地方人民政府関係部門のサイバーセキュリティ保護および監督管理職責は、国の関連規定に従って確定する。

第十条　ネットワーク運営者は、経営およびサービス活動の展開において、法律、行政法規を遵守し、社会公徳を尊重し、商業道徳を遵守し、信義則をもってサイバーセキュリティ保護義務を履行し、政府と社会による監督を受入れ、社会的責任を負うものとする。

第十一条　ネットワークの構築、運営ネットワークを通じてサービスを提供する場合、法律、行政法規の規定および国家標準の強制的要求に基づき、技術措置およびその他必要な措置を講じ、ネットワークの安全で安定的な運用を保障し、サイバーセキュリティインシデントに効果的に対応し、サイバー犯罪活動を防止し、ネットワークデータの完全性、機密性および可用性を維持しなければならない。

第十二条　ネットワーク関連業界の組織は、定款に基づいて業界の自律を強化し、サイバーセキュリティ行為の規範を制定し、成員のサイバーセキュリティ保護の強化を指導し、サイバーセキュリティの保護レベルを高め、業界の健全な発展を促進する。

第十三条　国は、公民、法人およびその他組織の法によるネットワーク使用権を保護し、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レベルを引上げ、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よる秩序ある自由な流動を保障する。

いかなる個人や組織も、ネットワーク使用において憲法と法律を遵守し、公共秩序を遵守し、社会の公徳を尊重しなければならず、またネットワークの安全を脅かしてはならず、ネットワークを利用した国家の安全や栄誉および利益を害する行為、国家政権転覆、社会主義制度の転覆扇動、国家分裂扇動、国家統一の破壊、テロリズムや過激主義の宣伝、民族憎悪や民族差別の宣伝、暴力やわいせつ・ポルノ情報の伝播、虚偽情報の捏造や伝播により経済秩序と社会秩序を乱す行為、他人の名誉やプライバシーおよび知的財産権またはその他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。

第十四条　国は未成年者の健全な成長に役立つネットワーク製品およびサービスの研究開発を支持し、未成年者の心身の健康を脅かすインターネットを利用した活動への従事を法によって処罰し、未成年者に安全かつ健全なネットワーク環境を提供する。

第十五条　いかなる個人および組織も、ネットワークの安全を脅かす行為をインターネット情報、電信、公安などの部門に通報する権利を有する。通報を受けた部門は法により遅滞なく処理しなければならない、通報を受けた部門の職責に属さない場合、処理権を有する部門に遅滞なく移送しなければならない。

関係部門は通報者の関連情報を秘密保持し、通報者の合法的権益を保護しなければならない。

第二章　サイバーセキュリティの支持および促進

第十六条　国は、サイバーセキュリティ規格の体系化を確立し、完全なものとする。国務院の標準化行政主管部門および国務院のその他関係部門は、各自の職責に基づき、サイバーセキュリティ管理およびネットワーク製品、サービスおよびセキュリティ運用に関する国家標準、業界標準の制定および適時改訂を組織する。

国は、企業、研究機関、高等教育機関、ネットワーク関連業界組織によるサイバーセキュリティ国家標準、業界標準の制定への参与を支持する。

第十七条　国務院および省・自治区・直轄市人民政府は、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および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および応用を支持し、安全で信頼できるネットワーク製品およびサービスを普及し、ネットワーク技術の知的財産権を保護し、企業、研究機関、高等教育機関などによる国家サイバーセキュリティ技術イノベーションプロジェクトへの参与を支持しなければならない。

第十八条　国はサイバーセキュリティの社会化サービス体系の構築を推進し、関連企業・機構がサイバーセキュリティ認証、テストおよびリスク評価などのセキュリティサービスを展開することを奨励する。
第十九条　国はネットワークデータのセキュリティ保護および利用技術の開発を奨励し、公共データ資源の開放を促進し、技術イノベーションおよび経済社会の発展を推進する。
第二十条　国は人工知能の基礎理論研究およびアルゴリズムなどの重要技術の研究開発を支持し、トレーニングデータのリソースやコンプティング・パワーなどのインフラストラクチャ構築を推進し、人工知能の倫理規範を整備し、リスクモニタリング評価とセキュリティ監督管理を強化し、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式のイノベーションを支持し、人工知能などの新技術を活用し、サイバーセキュリティの保護レベルを引き上げる。
第二十一条　各級人民政府およびその関連部門は、経常的なサイバーセキュリティ啓発教育を組織・展開し、かつ関係機関がサイバーセキュリティ啓発教育業務を適切に行うよう指導、督促しなければならない。
　マスメディアは、社会に向けて対象を絞ったサイバーセキュリティの啓発教育を行うべきである。
第二十二条　国は、企業および高等教育機関、職業学校などの教育訓練機構によるサイバーセキュリティ関連の教育および研修の展開を支持し、多種方式を採用してサイバーセキュリティ人材を育成し、サイバーセキュリティ人材の交流を促進する。

第三章　ネットワーク運用の安全

第一節　一般規定

第二十三条　国は、サイバーセキュリティ等級保護制度を実行する。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要求に従い、次の各号に掲げるセキュリティ保護義務を履行し、ネットワークが妨害、破壊または不正アクセスを受けないことを保障し、ネットワークデータ漏洩もしくは窃取、改ざんを防止しなければならない。
（一）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責任者を確定し、サイバーセキュリティ保護責任を実行する。
（二）コンピュータウイルスおよびサイバー攻撃、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措置を講じる。
（三）ネットワークの運用状態やセキュリティインシデントをモニタリング・記録する技術的措置を講じ、規定に従い関連するネットワークログを 6 か月以上保存する。
（四）データ分類、重要データのバックアップおよび暗号化などの措置を講じる。
（五）法律、行政法規に規定されたその他の義務。
第二十四条　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合致していなければならない。ネットワーク製品、サービス提供者は悪意のあるプログラムを設定してはならない。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が存在することを発見した場合、直ちに救済措置を講じ、規定に基づき遅滞なくユーザーに告知し、かつ関係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、サービスのため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。規定または当事者が約定した期限内に、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。
　ネットワーク製品、サービスがユーザー情報収集機能を有する場合、その提供者はユーザーにこれを明示すると共に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場合は、本法および関連法律、行政法規の個人情報保護に関する規定も遵守しなければならない。
第二十五条　基幹ネットワーク機器およびサイバーセキュリティ専用製品は、関連する国家標準の強制的要求に基づき、資格を備えた機関の安全認証に合格する、もしくは安全試験の要求

に合致した後、初めて販売または提供することができる。国家インターネット情報部門は国務院の関係部門と共同でネットワークの重要設備およびサイバーセキュリティ専用製品目録を制定、公布するとともに、安全認証および安全試験結果の相互承認を推進し、認証および検査の重複を回避する。

第二十六条　ネットワーク運営者がユーザーのために、ネットワークアクセス、ドメイン名登録サービスを行い、固定電話、携帯電話などのネットワーク接続手続き、もしくはユーザーへの情報公表やインスタントメッセージなどのサービスを提供する場合、ユーザーとの契約締結またはサービス提供を確認する際には、ユーザーに真実の身分情報提供を要求しなければならない。ユーザーが真実の身分情報を提供しない場合、ネットワーク運営者は関連サービスを提供してはならない。

国はネットワーク信頼アイデンティティ戦略を実施し、安全で便利なデジタルアイデンティティ認証技術の研究開発を支持し、異なるデジタルアイデンティティ認証の間の相互承認を推進する。

第二十七条　ネットワーク運営者は、サイバーセキュリティインシデントの緊急時対応策を制定し、システムの脆弱性、コンピュータウイルス、ネットワーク攻撃、ネットワーク侵入などのセキュリティリスクを遅滞なく処理しなければならない、ネットワークの安全を脅かすインシデントが発生した場合、直ちに緊急時対応策を発動し、相応しい救済措置を講じ、規定に基づき関係主管部門に報告する。

第二十八条　サイバーセキュリティ認証、テスト、リスク評価などの活動を展開し、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サイバーセキュリティ情報を社会に発表する場合は、国の関連規定を遵守しなければならない。

第二十九条　いかなる個人および組織も、他人のネットワークに不法侵入し、他人のネットワークの正常な機能を妨害し、ネットワークデータを窃取するなどのネットワークの安全を脅かす活動に従事してはならない。ネットワークへの侵入、ネットワークの正常な機能および防護措置の妨害、ネットワークデータの窃取などネットワークの安全を脅かす活動専用のプログラムやツールを提供してはならず、また他人がネットワークの安全を脅かす活動に従事することを知りながら、そのために技術サポート、広告普及、支払決済などの援助を提供してはならない。

第三十条　ネットワーク運営者は公安機関、国家安全機関が法に基づき国家の安全を維持し、犯罪捜査を行う活動に技術サポートと協力を提供しなければならない。

第三十一条　国は、ネットワーク運営者間のサイバーセキュリティ情報の収集、分析、通報および緊急対応処置などの面で協力し、ネットワーク運営者の安全保障能力を高めることを支持する。

関連業界組織は、当該業界のサイバーセキュリティ保護規範および協力メカニズムを構築・健全化し、サイバーセキュリティリスクに対する分析・評価を強化し、定期的に成員に対するリスク警告を行い、成員によるサイバーセキュリティリスクへの対応を支持しサポートする。

第三十二条　インターネット情報化部門および関連部門がサイバーセキュリティ保護職責の履行において取得した情報は、サイバーセキュリティの維持における必要にのみ用いることができ、その他の用途に使用してはならない。

第二節　重要情報インフラストラクチャの安全な運用

第三十三条　国は公共通信および情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政府などの重要な業界および分野、およびその他一度破壊、機能喪失またはデータ漏洩を受けた場合に国家安全、国の経済・民生、公共利益を深刻に脅かす可能性のある重要情報インフラストラクチャに対して、サイバーセキュリティ等級保護制度を基礎として、重点保護を実行する。重要情報インフラストラクチャの具体的な範囲とセキュリティ保護弁法は国務院が制定する。

国は、重要情報インフラストラクチャ以外のネットワーク運営者が自発的に重要情報インフラストラクチャ保護体系に参与することを奨励する。

第三十四条　国務院が定める職責分担に基づき、重要情報インフラストラクチャのセキュリティ保護業務に責任を負う部門は、当該業界・当該分野の重要情報インフラストラクチャのセキュリティ計画をそれぞれ作成し、組織・実施し、重要情報インフラストラクチャのセキュリティ運用保護業務を指導および監督する。
第三十五条　重要情報インフラストラクチャを構築するには、業務の安定・持続的な運行をサポートする性能を有することを確保し、かつ安全技術措置の同時計画・同時構築・同時使用を保証しなければならない。
第三十六条　重要情報インフラストラクチャの運営者は、本法第二十三条の規定のほか、次のセキュリティ保護義務を履行しなければならない。
（一）専門の安全管理機関および安全管理責任者を設置すると共に、当該責任者および重要職位の人員に対してセキュリティバックグラウンド審査を行う。
（二）従業員に対して定期的なサイバーセキュリティ教育、技術研修および技能考課を行う。
（三）重要なシステムとデータベースに対し、災害復旧バックアップを行う。
（四）サイバーセキュリティインシデントの緊急対応案を制定し、定期的に訓練を行う。
（五）法律、行政法規に規定されたその他の義務。
第三十七条　重要情報インフラストラクチャの運営者がネットワーク製品およびサービスを購入し、国家安全に影響が及ぶ可能性がある場合、国家インターネット情報部門が国務院の関連部門と共同で組織した国家安全審査を通過しなければならない。
第三十八条　重要情報インフラストラクチャの運営者はネットワーク製品およびサービスを購入する場合、規定に基づき提供者とセキュリティ秘密保持協定を締結し、セキュリティと秘密保持義務に関する責任を明確にしなければならない。
第三十九条　重要情報インフラストラクチャの運営者が中華人民共和国国内の運営において収集または生成した個人情報および重要データは、国内で保存しなければならない。業務の必要により、確かに国外に提供する必要がある場合、国家インターネット情報部門が国務院の関連部門と共同で制定した弁法に基づき安全評価を行わなければならない。法律、行政法規に別段の定めがある場合は、その規定に従う。
第四十条　重要情報インフラストラクチャの運営者は、自らまたはサイバーセキュリティサービス機構に委託し、そのネットワークの安全性および存在可能性のあるリスクに対して毎年少なくとも 1 回は試験・評価を実施すると共に、試験・評価の状況および改善措置を関連する重要情報インフラストラクチャのセキュリティ保護業務担当部門に報告を送らなければならない。
第四十一条　国家インターネット情報部門は、関連部門が重要情報インフラストラクチャのセキュリティ保護に対し、次の措置を講じるよう統一的に計画・調整しなければならない。
（一）重要情報インフラストラクチャのセキュリティリスクに対して抜取チェック・テストを行い、改善措置を提出し、必要に応じてサイバーセキュリティサービス機構にネットワークに存在するセキュリティリスクに対する試験・評価を委託することができる。
（二）定期的に重要情報インフラストラクチャの運営者を組織してサイバーセキュリティ緊急時対応実地訓練を行い、サイバーセキュリティインシデントへの対応レベルと協同協力能力を高める。
（三）関連部門・重要情報インフラストラクチャの運営者および関連研究機関・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情報共有を促進する。
（四）サイバーセキュリティインシデントの緊急対応処置とネットワーク機能のリカバリなどに対して、技術サポートと協力を提供する。

第四章　ネットワーク情報セキュリティ

第四十二条　ネットワーク運営者は、収集したユーザー情報を厳格に秘密保持し、健全なユーザー情報保護制度を確立しなければならない。
　ネットワーク運営者が個人情報を処理する場合、本法および『中華人民共和国民法典』、『中華人民共和国個人情報保護法』などの法律、行政法規の規定を遵守しなければならない。

第四十三条　ネットワーク運営者が個人情報を収集、使用する場合、合法、正当、必要の原則に従い、収集、使用規則を公開し、情報収集、使用の目的、方式および範囲を明示すると共に、被収集者の同意を得なければならない。

ネットワーク運営者は、その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、行政法規の規定および双方の約定に違反して個人情報を収集、使用してはならないと同時に、法律、行政法規の規定およびユーザーとの約定に基づき、その保存する個人情報を処理しなければならない。

第四十四条　ネットワーク運営者は、自身が収集した個人情報を漏洩、改ざん、毀損してはならない。被収集者の同意を得ずに、個人情報を他人に提供してはならない。ただし、処理を経て特定の個人を識別する方法がなく、かつ復元不能な場合を除く。

ネットワーク運営者は、技術的措置およびその他必要な措置を講じ、収集した個人情報セキュリティを確保し、情報の漏洩、毀損、紛失を防止しなければならない。個人情報の漏洩、毀損、紛失の状況が発生したもしくは発生可能性がある場合、直ちに救済措置を講じ、規定に基づき遅滞なくユーザーに告知し、かつ関係主管部門に報告しなければならない。

第四十五条　個人は、ネットワーク運営者が法律、行政法規の規定または双方の約定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。また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、ネットワーク運営者に訂正を要求する権利を有する。ネットワーク運営者は、削除もしくは訂正のための措置を講じなければならない。

第四十六条　いかなる個人および組織も、個人情報を窃取またはその他不法な方式で取得してはならず、個人情報を不法に販売もしくは不法に他人へ提供してはならない。

第四十七条　法によりサイバーセキュリティ監督管理の職責を負う部門およびその職員は、職責履行において知った個人情報、プライバシーおよび商業秘密を厳格に秘密保持しなければならず、漏洩、販売もしくは不法に他人へ提供してはならない。

第四十八条　いかなる個人および組織も、そのネットワーク使用行為に対して責任を負わなければならず、詐欺の実施、犯罪方法の伝授、違法禁止物品や規制対象物品の製作もしくは販売などの違法犯罪活動に用いるウェブサイトや通信グループを設立してはならず、インターネットを利用した詐欺の実施、違法禁止物品や規制対象物品の製作または販売その他の違法犯罪活動の情報を発表してはならない。

第四十九条　ネットワーク運営者は、そのユーザーが発表した情報に対する管理を強化し、法律、行政法規が発表もしくは伝送を禁止している情報を発見した場合、直ちに当該情報の伝送を停止し、消去などの処置措置を講じ、情報拡散を防止し、関連記録を保存すると共に関係主管部門に報告しなければならない。

第五十条　いかなる個人および組織が送信する電子情報、提供するアプリケーションソフトウェアにも、悪意のあるプログラムを設置してはならず、法律、行政法規が発表または伝送を禁止する情報を含んではならない。

電子情報送信サービス提供者およ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は、安全管理義務を履行し、そのユーザーに前項に定める行為があることを知った場合、サービス提供を停止し、消去処置などの措置を講じ、関連記録を保存すると共に関係主管部門に報告しなければならない。

第五十一条　ネットワーク運営者は、ネットワーク情報セキュリティに関する苦情・通報制度を構築し、苦情・通報方式などの情報を公布し、ネットワーク情報セキュリティに関する苦情および通報を遅滞なく受理し、処理しなければならない。

ネットワーク運営者は、インターネット情報化部門および関連部門が法により実施する監督検査に協力しなければならない。

第五十二条　国家インターネット情報部門および関連部門は法に基づきネットワーク情報セキュリティの監督管理職責を履行し、法律・行政法規が公布または伝送を禁止する情報を発見した場合、ネットワーク運営者に対し、伝送停止、消去処置などの措置を講じ、関連記録を保存するよう要求しなければならない、中華人民共和国国外から送られる上述の情報については、

関連する機関に対し、技術措置およびその他必要な措置を講じて伝播を遮断するよう通知しなければならない。

第五章　モニタリング・早期警報および緊急対応処置

第五十三条　国は、サイバーセキュリティのモニタリング・早期警報および情報通報制度を確立する。国家インターネット情報部門は、関連部門と統一的に協調してサイバーセキュリティ情報の収集・分析および通報業務を強化し、規定に基づきサイバーセキュリティのモニタリング・早期警報情報を統一的に発表しなければならない。

第五十四条　重要情報インフラストラクチャのセキュリティ保護業務に責任を負う部門は、当該業界・当該分野のサイバーセキュリティのモニタリング・早期警報および情報通報制度を構築・健全化し、かつ規定に従ってサイバーセキュリティのモニタリング・早期警報情報を報告送信しなければならない。

第五十五条　国家インターネット情報部門は関連部門と協調してサイバーセキュリティリスク評価および緊急対応業務メカニズムを構築・健全化し、サイバーセキュリティインシデント緊急対応対策案を制定し、定期的に実地訓練を組織する。

重要情報インフラストラクチャのセキュリティ保護業務を担当する部門は、当該業界、当該分野のサイバーセキュリティインシデント緊急対応対策事前案を制定すると共に、定期的に実地訓練を組織しなければならない。

サイバーセキュリティインシデント緊急対応対策事前案は、インシデント発生後の危害の程度、影響範囲などの要素に基づきサイバーセキュリティインシデントに対して等級付けを行うと共に、相応しい緊急対応処置の措置を規定しなければならない。

第五十六条　サイバーセキュリティインシデントの発生リスクが増大した場合、省級以上の人民政府の関係部門は規定の権限およびプロセスに従うと共に、サイバーセキュリティリスクの特徴と発生する可能性のある危害に基づいて、以下の措置を講じなければならない。

（一）関係する部門、機構および人員に対し遅滞なく関連情報を収集、報告し、サイバーセキュリティリスクに対するモニタリングを強化するよう要求する。

（二）関係する部門、機構および専門人員を組織し、サイバーセキュリティリスク情報に対して分析評価を行い、インシデントの発生可能性、影響範囲および危害の程度を予測する。

（三）社会に向けてサイバーセキュリティリスク早期警報を発表し、危害を回避、軽減する措置を公布する。

第五十七条　サイバーセキュリティインシデントが発生した場合、直ちにサイバーセキュリティインシデント緊急対応対策事前案を始動し、サイバーセキュリティインシデントに対して調査と評価を進め、ネットワーク運営者に技術措置およびその他必要な措置を講じ、セキュリティ上の潜在リスクを取り除き、危害拡大を防止するよう要求すると共に、公衆に関連する警告情報を遅滞なく社会に発表しなければならない。

第五十八条　省級以上の人民政府の関係部門は、サイバーセキュリティ監督管理の職責の履行において、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、もしくはセキュリティインシデントが発生したことを発見した場合、規定の権限およびプロセスに従い、当該ネットワーク運営者の法定代表者または主要責任者に対して面談を行うことができる。ネットワーク運営者は要求に従い措置を講じ、改善を進め、潜在リスクを取り除かなければならない。

第五十九条　サイバーセキュリティインシデントにより、突発的なインシデントまたは生産安全上の事故が発生した場合、『中華人民共和国突発事件対応法』、『中華人民共和国安全生産法』などの関連法律、行政法規の定めに従って処置しなければならない。

第六十条　国家安全と社会公共秩序を維持し、重大で突発的な社会セキュリティインシデントを処理する必要がある場合、国務院の決定もしくは認可を経て、特定区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。

第六章　法的責任

第六十一条　ネットワーク運営者が本法第二十三条、第二十七条に定めるサイバーセキュリティ保護義務を履行しない場合、関係主管部門が是正を命じ、警告を与え、1 万元以上 5 万元以下の罰金を科すことができる。是正を拒否する、もしくはネットワークの安全を脅かすなどの結果をもたらした場合、5 万元以上 50 万元以下の罰金を科し、直接責任を負う主管者およびその他の直接責任者に対しては 1 万元以上 10 万元以下の罰金を科す。

重要情報インフラストラクチャの運営者が本法第三十五条、第三十六条、第三十八条、第四十条に定めるサイバーセキュリティ保護義務を履行しない場合、関係主管部門が是正を命じ、警告を与え、5 万元以上 10 万元以下の罰金を科すことができる。是正を拒否する、もしくはネットワークの安全を脅かすなどの結果をもたらした場合、10 万元以上 100 万元以下の罰金を科し、直接責任を負う主管者およびその他直接責任者に対して 1 万元以上 10 万元以下の罰金を科す。

前 2 項の行為があり、大量のデータ漏洩、重要情報インフラストラクチャの一部機能喪失などネットワークの安全を深刻に脅かす結果をもたらした場合、関係主管部門は 50 万元以上 200 万元以下の罰金を科し、直接責任を負う主管者およびその他直接責任者に対して 5 万元以上 20 万元以下の罰金を科す。重要情報インフラストラクチャの主要機能喪失などネットワークの安全を特に深刻に脅かす結果をもたらした場合、200 万元以上 1 千万元以下の罰金を科し、直接責任を負う主管者およびその他直接責任者に対して 20 万元以上 100 万元以下の罰金を科す。

第六十二条　本法第二十四条第一項、第二項および第五十条第一項の定めに違反し、次の行為のいずれかに該当する場合、関係主管部門が是正を命じ、警告を与える。是正を拒否する、もしくはネットワークの安全を脅かすなどの結果をもたらした場合、5 万元以上 50 万元以下の罰金を科し、直接責任を負う主管者に対して 1 万元以上 10 万元以下の罰金を科す。

（一）悪意のあるプログラムを設定した場合。

（二）その製品、サービスに存在するセキュリティ上の欠陥、脆弱性などのリスクに対して直ちに救済措置を講じていない、もしくは規定に従って遅滞なくユーザーに告知していないと同時に関係主管部門に報告していない場合。

（三）無断でその製品、サービスに対するセキュリティメンテナンスの提供を終了した場合。

前項第一項、第二項の行為があり、本法第六十一条第三項に定める結果をもたらした場合、当該項の規定に基づき処罰する。

第六十三条　本法第二十五条の規定に違反し、安全認証、安全試験を経ていない、もしくは安全認証に不合格、安全試験で要件に合致しない基幹ネットワーク機器およびサイバーセキュリティ専用製品を販売または提供した場合、関係主管部門が販売もしくは提供の停止を命じ、警告を与え、違法所得を没収する。違法所得がない、もしくは違法所得が 10 万元未満の場合、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、違法所得の 1 倍以上 5 倍以下の罰金を併科する。情状が重大である場合は、関連業務の一時停止、問題是正のための業務停止、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、その規定に従う。

第六十四条　ネットワーク運営者が本法第二十六条第一項の定めに違反し、ユーザーに真実の身分情報の提供を要求していない、または真実の身分情報を提供しないユーザーに対して関連サービスを提供した場合、関係主管部門は是正を命じる。是正を拒否する、もしくは情状が深刻な場合、5 万元以上 50 万元以下の罰金を科すと共に、関連業務の一時停止、問題是正のための業務停止、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およびその他直接責任者に対して 1 万元以上 10 万元以下の罰金を科すことができる。

第六十五条　本法第二十八条の定めに違反し、サイバーセキュリティ認証、セキュリティテスト、リスク評価などの活動を展開し、またはシステムの脆弱性、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社会に発表した場合、関係主

管部門が是正を命じ、警告を与え、1 万元以上 10 万元以下の罰金を科すことができる。是正を拒否する、もしくは情状が深刻な場合、10 万元以上 100 万元以下の罰金を科し、かつ関連業務の一時停止、問題是正のための業務停止、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およびその他の直接責任者に対して 1 万元以上 10 万元以下の罰金を科すことができる。

前項の行為があり、本法第六十一条第三項に定める結果をもたらした場合、同項の規定に従って処罰する。

第六十六条 本法第二十九条の定めに違反し、ネットワークの安全を脅かす活動に従事した、もしくはネットワークの安全を脅かす活動専用のプログラムやツールを提供した、もしくは他人がネットワークの安全を脅かす活動に従事するために技術サポート、広告普及、支払決済などの援助を提供した場合において、犯罪を構成しない場合、公安機関が違法所得を没収し、5 日以下の拘留に処し、5 万元以上 50 万元以下の罰金を併科することができる。情状が比較的重い場合、5 日以上 15 日以下の拘留に処し、10 万元以上 100 万元以下の罰金を併科することができる。

組織に前項の行為がある場合、公安機関は違法所得を没収し、10 万元以上 100 万元以下の罰金に処し、かつ直接責任を負う主管者およびその他の直接責任者に対して前項の規定に基づき処罰する。

本法第二十九条の規定に違反し、治安管理処罰を受けた人員は、5 年以内にサイバーセキュリティ管理およびネットワーク運営の重要な職位の業務に従事してはならない。刑事処罰を受けた者は、サイバーセキュリティ管理およびネットワーク運営の重要な職位の業務に終身にわたり従事してはならない。

第六十七条 重要情報インフラストラクチャの運営者が本法第三十七条の定めに違反し、安全審査を経ていないもしくは安全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、購入金額相当以上 10 倍以下の罰金を科し、直接責任を負う主管者およびその他の直接責任者に対して 1 万元以上 10 万元以下の罰金を科す。

第六十八条 本法第四十八条の定めに違反し、違法犯罪活動の実施に用いるウェブサイト、通信グループを設立し、またはインターネットを利用して違法犯罪活動の実施に関わる情報を発表し、犯罪を構成しない場合、公安機関が 5 日以下の拘留に処し、1 万元以上 10 万元以下の罰金を併科することができる。情状が比較的重い場合、5 日以上 15 日以下の拘留に処し、5 万元以上 50 万元以下の罰金を併科することができる。違法犯罪活動を実施するためのウェブサイト、通信グループは閉鎖する。

組織に前項の行為がある場合、公安機関は 10 万元以上 50 万元以下の罰金を科すと共に、直接責任を負う主管者およびその他の直接責任者に対して前項の定めに従い処罰する。

第六十九条 ネットワーク運営者が本法第四十九条の定めに違反し、法律・行政法規が公布または伝送を禁止する情報の伝送を停止せず、除去処置などの措置を講じず、関連記録の保存や関係主管部門への報告をしない場合、もしくは本法第五十二条の定めに違反し、関連部門の要求に従って法律・行政法規が公布または伝送を禁止している情報の伝送を停止せず、除去処置などの措置を講じず、関連記録を保存しない場合、関係主管部門が是正を命じ、警告を与え、通報し、5 万元以上 50 万元の罰金を科すことができる。是正を拒否する、もしくは情状が深刻な場合、50 万元以上 200 万元以下の罰金を科し、かつ関連業務の一時停止、問題是正のための業務停止、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およびその他の直接責任者に対して 5 万元以上 20 万元以下の罰金を科すことができる。

前項の行為があり、特に重大な影響、特に重大な結果をもたらした場合、関係主管部門は 200 万元以上 1 千万元以下の罰金を科し、関連業務の一時停止、問題是正のための業務停止、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およびその他直接責任者に対して 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、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定める安全管理義務を履行しない場合、前 2 項の規定に従って処罰する。

第七十条　ネットワーク運営者が本法の定めに違反し、次の行為のいずれかに該当する場合、関係主管部門が是正を命じる。是正を拒否する、もしくは情状が深刻な場合、5 万元以上 50 万元以下の罰金を科し、直接責任を負う主管者およびその他直接責任者に対して 1 万元以上 10 万元以下の罰金を科す。

（一）関係部門が法に依って実施する監督検査を拒絶、妨害した場合。

（二）公安機関、国家安全機関に技術サポートと協力を提供しない場合。

第七十一条　次の行為のいずれかに該当する場合、関連法律、行政法規の規定に従って処理、処罰する。

（一）本法第十三条第二項およびその他の法律、行政法規が公布または伝送を禁止する情報を公布または伝送した場合。

（二）本法第二十四条第三項、第四十三条から第四十五条の定めに違反し、個人情報の権益を侵害した場合。

（三）本法第三十九条の定めに違反し、重要情報インフラストラクチャの運営者が国外で個人情報および重要データを保存し、または国外に個人情報および重要データを提供した場合。

本法第四十六条の定めに違反し、個人情報を窃取したもしくはその他の不法方式により取得、不法販売または不法に他人に提供した場合において、犯罪を構成しない場合、公安機関は関連法律、行政法規の規定に従って処罰する。

第七十二条　本法に定める違法行為がある場合、関連法律、行政法規の規定に基づき信用档案に記入すると共に公示する。

第七十三条　本法の定めに違反するが、『中華人民共和国行政処罰法』に定める、軽きに従う処罰、処罰軽減または不処罰の状況がある場合、その規定に基づき軽きに従う処罰、処罰軽減または不処罰とする。

第七十四条　国家機関の政務ネットワークの運営者が本法に定めるサイバーセキュリティ保護義務を履行しない場合、その上級機関または関連機関が是正を命じる。直接責任を負う主管者およびその他直接責任者に対しては、法により処分を与える。

第七十五条　インターネット情報化部門および関連部門が本法第三十二条の定めに違反し、サイバーセキュリティ保護職責の履行において取得した情報をその他の用途に用いる場合、直接責任を負う主管者およびその他直接責任者に対して法により処分を与える。

インターネット情報化部門および関係部門の職員が職務怠慢、職権濫用、私利をはかり不正を働き、犯罪を構成しない場合、法により処分を与える。

第七十六条　本法の定めに違反し、他人に損害を与えた場合、法により民事責任を負う。

本法の定めに違反し、治安管理違反行為を構成する場合、法により治安管理処罰を与える。犯罪を構成する場合、法により刑事責任を追及する。

第七十七条　国外の機構、組織、個人が中華人民共和国のネットワークの安全を脅かす活動に従事する場合、法により法的責任を追及する。重大な結果をもたらした場合、国務院公安部門および関係部門は、当該機構、組織、個人に対して財産凍結もしくはその他必要な制裁措置を講じることを決定することができる。

第七章　附　則

第七十八条　本法の次の用語の意味は以下の通りとする。

（一）ネットワークとは、コンピュータまたは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従って情報を収集、保存、伝送、交換、処理するシステムをいう。

（二）サイバーセキュリティ（ネットワークの安全）とは、必要な措置を講じることにより、ネットワークに対する攻撃、侵入、妨害、破壊および不法使用および不慮の事故を防止し、ネ

ットワークを安定した信頼性の高い運行状態にし、またネットワークデータの完全性、機密性、可用性を保障する能力をいう。
（三）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提供者をいう。
（四）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、処理および生成された各種電子データをいう。
（五）個人情報とは、電子またはその他の方式で記録された単独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することができる自然人の氏名、生年月日、身分証明書番号、個人生体識別情報、住所、電話番号などを含むがこれらに限定されない各種情報をいう。
第七十九条　国家秘密情報に関わるネットワークの保存、処理のセキュリティ運用保護は、本法を遵守しなければならないほか、秘密保持法律、行政法規の定めも遵守しなければならない。
第八十条　軍事ネットワークのセキュリティ保護については、中央軍事委員会が別途定めるものとする。
第八十一条　本法は 2017 年 6 月 1 日より施行する。

