中华人民共和国网络安全法

ネットワーク安全法

第 1 章　总则

第 1 条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第 2 条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第 3 条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第 4 条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第 5 条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第 6 条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第 7 条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合

第 1 章　総則

第 1 条 ネットワークの安全を保障し、ネットワーク空間の主権並びに国の安全及び社会の公共の利益を保ち、公民、法人その他の組織の適法な権益を保護し、なお且つ経済・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 2 条 中華人民共和国内におけるネットワークの建設、運営、維持・保護、使用並びにネットワークの安全の監督管理について、本法を適用する。

第 3 条 国は、ネットワークの安全と情報化の発展をともに重んじ、積極的な利用、合理的な発展、法による安全を管理・保証する方針を遵守し、ネットワークのインフラストラクチャーの建設及び相互接続を推進し、ネットワーク技術のイノベーション及び応用を奨励し、ネットワークの安全に関わる人材の養成をサポートし、ネットワークの安全を保障する体系を確立して整備し、ネットワークの安全を保護する能力を引き上げる。

第 4 条 国は、ネットワークの安全戦略を制定して絶えず改善してゆき、ネットワークの安全の保障にかかる基本的要求及び主たる目標を明確にし、重点分野におけるネットワークの安全政策、業務任務及び措置を提起する。

第 5 条 国は、措置を講じて、中華人民共和国の国内外からもたらされるネットワークの安全上のリスク及び脅威をモニタリング、防御、処置し、重要情報のインフラストラクチャーが攻撃、侵入、妨害、破壊を受けないよう保護し、法によりネットワークに対する違法な犯罪行為を厳しく取り締まり、ネットワーク空間の安全及び秩序を維持・保護する。

第 6 条 国は、信義誠実かつ健全・文明的なネットワークの利用を提唱し、社会主義の根幹をなす価値観の普及を図り、措置を講じて社会全体のネットワークの安全に対する意識及びレベルを引き上げ、社会全体がネットワークの安全に共同で参与しこれを促進するという望ましい環境を形成する。

第 7 条 国は、ネットワーク空間の整備、ネットワーク技術の研究開発及び基準の制定、ネットワーク

作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

に対する違法な犯罪の取締り等の面で国際交流及び提携を積極的に行い、平和、安全、開放、提携のネットワーク空間の構築を推進し、多方面にわたり、民主的で透明なネットワーク整備システムを確立する。

第 8 条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第 8 条 国のネットワーク安全情報化機関は、ネットワークの安全業務及び関連監督管理業務の統一的な調整に責任を負う。国務院の電信所管機関、公安機関その他の関係機関は、本法並びに関係する法律及び行政法規の規定により、各自の職責の範囲でネットワークの安全の保護及び監督管理業務に責任を負う。

県級以上の地方人民政府の関係機関のネットワークの安全保護及び監督管理の職責は、国の関係規定に従い、これを確定する。

第 9 条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

第 9 条 ネットワークプロバイダは、経営及びサービス活動を展開するにあたり、法律及び行政法規を遵守し、社会道徳を尊重し、商業倫理を遵守し、信義則を守り、ネットワークの安全保護の義務を履行し、政府及び社会の監督を受け、社会的な責任を負わなければならない。

第 10 条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第 10 条 ネットワークを建設するか運営するか、ネットワークを通じてサービスを提供するにあたっては、法律及び行政法規の規定並びに国家の基準の強制的な要請により、技術的措置その他の必要な措置を講じ、ネットワークの安全且つ安定的な運行を保障し、ネットワークの安全を脅かす事件へ有効に対処し、ネットワークに対する違法な犯罪行為を防止し、ネットワークデータの完全性、秘密保持性とユーザビリティを維持・保護しなければならない。

第 11 条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第 11 条 ネットワークの関連業界団体は、定款に従い、業界の自律性を強化し、ネットワークの安全を脅かす行為に対する制度を制定し、会員をネットワークの安全保護を強化するよう指導し、ネットワークの安全保護の水準を引き上げ、業界の健全な発展を促進する。

第 12 条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

第 12 条 国は、公民、法人その他の組織が法によりネットワークを使用することにかかる権利を保護し、ネットワークの接続の普及を促進し、ネットワークサービスの水準を引き上げ、社会に安全且つ便利なネットワークサービスを提供し、ネットワーク

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

情報が法により秩序を持って自由に流通することを保障する。

いかなる個人及び組織も、ネットワークを使用するにあたり、憲法・法律を遵守し、公の秩序を遵守し、社会道徳を尊重しなければならず、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て国の安全、栄誉、利益を脅かし、国家政権の転覆及び社会主義制度の転覆を煽動し、国の分裂及び国家統一を破壊することを煽動し、テロリズム及び過激主義を宣揚し、民族に対する憎悪や差別を宣揚し、暴力及びわいせつな情報を流布し、虚偽情報を捏造、散布して経済の秩序及び社会秩序を撹乱し、他人の名誉、プライバシー、知的財産権その他の適法な権益を侵害する等の活動に従事してはならない。

第 13 条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第 13 条 国は、未成年者の健全な成長に資するネットワーク製品及びサービスの研究開発をサポートし、ネットワークを利用して未成年者の心身の健康を損なう活動に従事することを法により厳しく取り締まり、未成年者のため安全且つ健全なネットワーク環境を提供する。

第 14 条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第 14 条 いかなる個人及び組織も、ネットワークの安全を脅かす行為についてネットワークの安全及び情報化、電信、公安等の機関に対し通報する権利を持つ。通報を受けた機関は、遅滞なく法に従って処理をしなければならない。当該機関の職責に属さない場合には、遅滞なく処理の権限を持つ機関に送致しなければならない。

関係機関は、通報者の関連情報について秘密を保持し、通報者の適法な権益を保護しなければならない。

第 2 章　网络安全支持与促进

第 2 章　ネットワークの安全に対するサポートと促進

第 15 条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第 15 条 国は、ネットワークの安全基準システムを確立し、完全化する。国務院標準化行政所管機関及び国務院のその他の関係機関は、各自の職責に基づき、ネットワークの安全管理並びにネットワーク製品、サービス及び運行の安全に関する国家基準及び業界基準の制定並びに適時の改正を実施する。

国は、企業、研究機関、大学・大学院、ネットワーク関連業界団体がネットワークの安全の国家基準及び業界基準の制定に参与することをサポート

する。

第 16 条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

第 16 条 国務院並びに省、自治区及び直轄市の人民政府は、全体計画を取りまとめて取り組みを強化し、重点的なネットワークの安全技術産業及びプロジェクトを支援し、ネットワークの安全技術の研究開発及び応用を支持し、安全且つ信頼できるネットワーク製品及びサービスを普及させ、ネットワーク技術にかかる知的財産権を保護し、企業、研究機関及び大学・大学院等が国のネットワークの安全技術のイノベーションプロジェクトに参与することをサポートしなければならない。

第 17 条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第 17 条 国は、ネットワークの安全の社会化サービスシステムの構築を推進し、関係企業及び機関がネットワークの安全の認証、検査測定及びリスク評価等の安全サービスを展開することを奨励する。

第 18 条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

第 18 条　国は、ネットワークデータの安全の保護及び利用技術の開発を奨励し、公共データソースの開放を促進し、技術イノベーション及び経済社会の発展を促進する。

国は、ネットワークの安全の管理方式のイノベーションを支持し、ネットワークの新技術を運用し、ネットワークの安全の保護水準を引き上げる。

第 19 条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第 19 条 各級の人民政府及びその関係機関は、経常的なネットワークの安全の宣伝教育を実施統括し、なお且つ関係機関・組織がネットワークの安全の宣伝教育業務を適切に遂行するよう指導し、督促しなければならない。

マスメディアは、社会に対して目的に適合したネットワークの安全に関する宣伝教育を行わなければならない。

第 20 条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第 20 条 国は、企業及び大学・大学院、職業学校等の教育研修機関がネットワークの安全に関連した教育及び研修を展開することをサポートし、様々な方法を採用してネットワークの安全にかかる人材を養成し、ネットワークの安全にかかる人材の交流を促進する。

第 3 章　网络运行安全
第 1 節　一般规定

第 3 章　ネットワーク運行上の安全
第 1 節　一般規定

第 21 条 国家实行网络安全等级保护制度。网络运营

第 21 条 国は、ネットワークの安全のランク保護制

者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

度を実施する。ネットワークプロバイダは、ネットワークの安全のランク保護制度の要求に従い、次に掲げる安全保護義務を履行し、ネットワークが妨害、破壊されたり、授権されていないアクセスを受けることがないよう保障し、ネットワークデータが漏えいするか、窃取されるか、改竄されることを防止しなければならない。

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

(1) 内部安全管理制度及び操作規程を制定し、ネットワークの安全責任者を確定し、ネットワークの安全にかかる保護責任の確実な履行をはかる。

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

(2) コンピューターウィルス及びサイバー攻撃、ネットワーク侵入等のネットワークの安全を脅かす行為を防止する技術的な措置を講じる。

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

(3) ネットワークの運行状態及びネットワークの安全にかかる事件のモニタリング及び記録にかかる技術措置を講じ、なお且つ規定に従い関連するネットワークのログを少なくとも 6 箇月間は保存する。

（四）采取数据分类、重要数据备份和加密等措施；

(4) データ分類並びに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。

（五）法律、行政法规规定的其他义务

(5) その他、法律及び行政法規に定める義務

第 22 条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第 22 条 ネットワーク製品及びサービスは、関連する国家基準の強制的な要請に適合するものとしなければならない。ネットワーク製品及び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。そのネットワーク製品及びサービスに安全上の欠陥、セキュリティホール等のリスクが存在することを発見した際には、直ちに救済措置を講じ、規定に従い遅滞なく使用者に告知し、なお且つ関係所管機関に対し報告しなければならない。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

ネットワーク製品及びサービスの提供者は、その製品及びサービスのため安全の維持・保護を持続的に提供しなければならない。所定又は当事者が約定する期間においては、安全の維持・保護の提供を終了してはならない。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

ネットワーク製品及びサービスに使用者情報の収集の機能がある場合、その提供者は、使用者に対しこれを明示し、なお且つ同意を得なければならない。使用者の個人情報に関わる場合は、更に本法並びに関係する法律及び行政法規の個人情報保護に

关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

関する規定を遵守しなければならない。

第 23 条 ネットワークの重要設備及びネットワークの安全専用製品は、関連する国家基準の強制的な要請に従い、資格を具備する機関の安全認証に合格するか、安全検査測定が要求に適合した場合に限り、これらを販売するか、提供することができる。国のネットワーク安全情報化機関は、国務院の関係機関と共同してネットワーク重要設備及びネットワークの安全の専用製品目録を制定、公表、なお且つ安全認証及び安全検査測定結果の相互認証を推進し、認証及び検査測定の重複を回避する。

第 24 条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

第 24 条 ネットワークプロバイダは、使用者のためにネットワークの接続及びドメイン名登録の手続を行い、固定電話、移動体通信等のネットワーク接続手続を行うか、使用者のために情報の頒布、インスタントメッセンジャー等のサービスを提供するにあたり、使用者と協議を締結するか、サービスの提供を確認する際に、使用者に真実の身分情報を提供するよう要求しなければならない。使用者が真実の身分情報を提供しない場合、ネットワークプロバイダは、当該使用者のために関連サービスを提供してはならない。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

国は、ネットワーク身分信頼戦略を実施し、安全で便利な電子身分認証技術の研究開発をサポートし、異なる電子身分認証の間の相互認証を推進する。

第 25 条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第 25 条 ネットワークプロバイダは、ネットワークの安全にかかる事件のための緊急対応マニュアルを制定し、遅滞なくシステムのセキュリティホール、コンピューターウィルス、サイバー攻撃、ネットワーク侵入等の安全にかかるリスクを処置しなければならない。ネットワークの安全を脅かす事件が発生した際には、直ちに緊急対応マニュアルをスタートさせ、相応の救済措置を講じ、なお且つ規定に従い関係所管機関に対し報告する。

第 26 条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第 26 条 ネットワークの安全認証、検査測定、リスク評価等の活動を展開し、社会に対しシステムのセキュリティホール、コンピューターウィルス、サイバー攻撃、ネットワーク侵入等のネットワークの安全情報を発表するにあたって、国の関係規定を遵守しなければならない。

第 27 条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第 27 条 いかなる個人及び組織も、他人のネットワークへ違法に侵入し、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等のネットワークの安全を脅かす活動に従事してはならず、ネットワークへの侵入、ネットワークの正常な機能及び防護措置の妨害、ネットワークデータの窃取等のネットワークの安全を脅かす活動への従事に専ら用いるプログラム及び手段を提供してはならない。他人がネットワークの安全を脅かす活動に従事していることを明らかに知っている場合には、当該他人のため技術サポート、広告普及、支払決済等の援助を提供してはならない。

第 28 条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第 28 条 ネットワークプロバイダは、公安機関及び国の安全機関のため法により国の安全及び犯罪捜査の活動を維持・保護し、技術サポート及び協力を提供しなければならない。

第 29 条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第 29 条 国は、ネットワークプロバイダ相互間でネットワークの安全情報の収集、分析、通報及び緊急対応処置等の面において協力し、ネットワークプロバイダの安全保障能力を引き上げることをサポートする。

関係する業界団体は、当該業界のネットワークの安全保護制度及び協力メカニズムを確立して整備し、ネットワークの安全にかかるリスクについての分析評価を強化し、定期的に会員へリスクに対する警告を行い、会員によるネットワークの安全にかかるリスクへの対応をサポートし、これに協力する。

第 30 条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第 30 条 ネットワーク安全情報化機関及び関係機関は、ネットワークの安全保護職責の履行において取得した情報について、これをネットワークの安全の維持・保護の必要にのみ使用することができるものとし、他の用途に使用してはならない。

第 2 節　关键信息基础设施的运行安全

第 2 節　重要情報インフラストラクチャーの運行の安全

第 31 条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

第 31 条 国は、公共通信及び情報サービス、エネルギー、交通、水利、金融、公共サービス、電子行政サービス等の重要業界及び分野や、一旦機能の破壊若しくは喪失又はデータ漏えいに遭遇すると、国の安全、国民の経済・生活及び公共の利益に重大な危害を及ぼす恐れおそれのある重要な情報インフラストラクチャーについて、ネットワークの安全ラン

ク保護制度に基づき、重点的な保護を実施する。重要情報インフラストラクチャーの具体的範囲及び安全保護弁法については、国務院がこれを制定する。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

国は、重要情報インフラストラクチャー以外のネットワークプロバイダが自由意思により重要情報インフラストラクチャー保護システムに参与することを奨励する。

第 32 条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

第 32 条 国務院が定める職責分担に従い、重要情報インフラストラクチャーの安全保護業務に責任を負う機関は、それぞれ当該業界及び当該分野の重要情報インフラストラクチャーにかかる安全計画を編成して実施し、重要情報インフラストラクチャーの運行安全保護業務を指導、監督する。

第 33 条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第 33 条 重要情報インフラストラクチャーの建設にあたっては、当該重要情報インフラストラクチャーが業務の安定的かつ持続的な運行をサポートする性能を持つことを確実に保証し、なお且つ安全技術措置の同時計画、同時建設、同時使用を保証しなければならない。

第 34 条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：
第 35 条

第 34 条 本法第 21 条の規定を除き、重要情報インフラストラクチャーの運営者は、次に掲げる安全保護義務を履行しなければならない。

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

(1) 専門の安全管理機関及び安全管理責任者を設置し、なお且つ当該責任者及び重要職位の人員に対し安全背景の審査を行う。

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

(2) 業務に従事する者に対し、定期的にネットワークの安全にかかる教育、技術研修及び技能考査を行う。

（三）对重要系统和数据库进行容灾备份；

(3) 重要なシステム及びデータベースについて災害に備えたバックアップをとる。

（四）制定网络安全事件应急预案，并定期进行演练；

(4) ネットワークの安全にかかる事件のための緊急対応マニュアルを制定し、なお且つ定期的に訓練を行う。

（五）法律、行政法规规定的其他义务。

(5) その他、法律及び行政法規所定の義務

第 35 条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门

第 35 条 重要情報インフラストラクチャーの運営者は、ネットワーク製品及びサービスを調達する場

会同国务院有关部门组织的国家安全审查。

合に、国の安全に影響をもたらすおそれのあるときは、国のネットワーク安全情報化機関が国務院の関係機関と共同して実施する国の安全審査に合格しなければならない。

第 36 条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第 36 条 重要情報インフラストラクチャーの運営者は、ネットワーク製品及びサービスを調達するにあたり、規定に従い提供者と安全秘密保持契約を締結し、安全及び秘密保持にかかる義務及び責任を明確化しなければならない。

第 37 条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。

因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第 37 条 重要情報インフラストラクチャーの運営者が中華人民共和国の国内での運営において収集、発生させた個人情報及び重要データは、国内で保存しなければならない。

業務の必要性により、国外に対し確かに提供する必要のある場合には、国のネットワーク安全情報化機関が国務院の関係機関と共同して制定する弁法に従い安全評価を行わなければならない。法律及び行政法規に別段の定めのある場合には、当該定めに基づいて行う。

第 38 条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第 38 条 重要情報インフラストラクチャーの運営者は、自ら又はネットワークの安全サービス機関に委託し当該重要情報インフラストラクチャーのネットワークの安全性及び存在するおそれのあるリスクについて、毎年少なくとも 1 回の検査測定評価を行い、なお且つ検査測定評価状況及び改善措置を関連する重要情報インフラストラクチャーの安全保護業務に責任を負う機関に送付し報告しなければならない。

第 39 条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

第 39 条 国のネットワーク安全情報化機関は、関係機関を統括して重要情報インフラストラクチャーの安全保護について次に掲げる措置を講じさせなければならない。

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

(1) 重要情報インフラストラクチャーの安全にかかるリスクについてサンプル検査・検査測定をし、改善措置を提出する。必要のある際には、ネットワークの安全サービス機関に委託しネットワークに存在する安全にかかるリスクについて検査測定評価をさせることができる。

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同

(2) 定期的に重要情報インフラストラクチャーの運営者によるネットワークの安全の緊急対応訓練

配合能力；

を実施し、ネットワークの安全にかかる事件に対応する水準及び協同・協力の能力を引き上げる。

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

(3) 関係機関、重要情報インフラストラクチャーの運営者及び関係する研究機関、ネットワークの安全サービス機関等の間のネットワークの安全情報の共有を促進する。

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

(4) ネットワークの安全にかかる事件の緊急対応処置及びネットワーク機能の回復等について、技術サポート及び協力を提供する。

第 4 章　网络信息安全

第 4 章　ネットワーク情報の安全

第 40 条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第 40 条 ネットワークプロバイダは、自らが収集した使用者の情報について厳格に秘密を保持し、なお且つ使用者情報の保護制度を確立して健全化しなければならない。

第 41 条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第 41 条 ネットワークプロバイダは、個人情報を収集、使用するにあたり、適法、正当及び必要の原則を遵守し、収集及び使用の規則を公開し、情報収集及び使用の目的、方法及び範囲を明示し、なお且つ提供者の同意を得なければならない。

ネットワークプロバイダは、自らが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、法律及び行政法規の規定並びに双方の約定に違反して個人情報を収集、使用してはならず、なお且つ法律及び行政法規の規定並びに使用者との約定により、自らが保存する個人情報を取り扱わなければならない。

第 42 条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第 42 条 ネットワークプロバイダは、自らが収集した個人情報を漏えい、改竄、毀損してはならない。提供者の同意を経ずに、他人に対し個人情報を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すべがなく、なお且つ復元不能である場合を除く。

ネットワークプロバイダは、技術的な措置その他の必要な措置を講じ、自らが収集した個人情報の安全を確実に保証し、情報の漏えい、毀損及び紛失を防止しなければならない。個人情報の漏えい、毀損又は紛失が発生するか、発生する恐れのある状況においては、直ちに救済措置を講じ、規定に従い遅滞なく使用者に告知し、なお且つ関係所管機関に対し

报告。

第 43 条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第 43 条 個人は、ネットワークプロバイダが法律、行政法規の規定又は双方の約定に違反して当該個人の個人情報を収集するか、使用したことを発見した場合には、ネットワークプロバイダに当該個人の個人情報の削除を要求する権利を持つ。ネットワークプロバイダが収集するか、保存する当該個人の個人情報に誤りのあることを発見した場合には、ネットワークプロバイダに更正を要求する権利を持つ。ネットワークプロバイダは、措置を講じて削除するか更正しなければならない。

第 44 条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第 44 条 いかなる個人及び組織も、個人情報を窃取するか、その他の不法な方式により、これを取得してはならず、個人情報を不法に販売するか、他人に対し不法に提供してはならない。

第 45 条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第 45 条 法によりネットワークの安全監督管理の職責を負う機関及びその職員は、必ず職責の履行において知り得た個人情報及びプライバシー並びに商業上の秘密を厳格に秘密保持しなければならず、これらを漏えい、販売、不法に他人に対し提供してはならない。

第 46 条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第 46 条 いかなる個人及び組織も、自らのネットワーク使用の行為について責任を負わなければならず、詐欺の実施、犯罪方法の伝授又は違法禁止物品若しくは規制物品等の製作若しくは販売等の違法な犯罪行為に用いるウェブサイト又は通信グループを設立してはならず、ネットワークを利用して詐欺を働いたり、違法禁止物品、規制物品の製作又は販売その他の違法な犯罪行為の情報を頒布したりしてはならない。

第 47 条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第 47 条 ネットワークプロバイダは、自らの使用者が頒布する情報についての管理を強化しなければならない。法律及び行政法規により頒布又は伝送が禁止される情報を発見した場合には、直ちに当該情報の伝送を停止し、消去等の処置措置を講じ、情報の拡散を防止し、関係記録を保存し、なお且つ関係所管機関に対し報告しなければならない。

第 48 条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

第 48 条 いかなる個人及び組織の発信する電子情報及び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

律及び行政法規により頒布又は伝送が禁止される情報を含んではならない。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关部门报告。

電子情報発信サービス提供者及び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、安全管理義務を履行しなければならず、その使用者が前項所定の行為をしたことを知った場合には、サービスの提供を停止し、消去等の処置措置を講じ、関係記録を保存し、なお且つ関係所管機関に対し報告しなければならない。

第 49 条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

第 49 条 ネットワークプロバイダは、ネットワーク情報安全にかかる苦情申立て及び通報の制度を確立し、苦情申立て、通報方式等の情報を公表し、遅滞なくネットワーク情報安全に関係する苦情申立て及び通報を受理し、なお且つ処理しなければならない。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

ネットワークプロバイダは、ネットワーク安全情報化機関及び関係機関が法により実施する監督検査に対し、協力をしなければならない。

第 50 条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

第 50 条 国のネットワーク安全情報化機関は、法によりネットワーク情報安全の監督管理の職責を履行するにあたり、法律及び行政法規により頒布又は伝送が禁止される情報を発見した場合には、ネットワークプロバイダに伝送を停止するよう要求し、消去等の処置措置を講じ、関係記録を保存しなければならない。中華人民共和国外からもたらされたそれらの情報については、技術措置及びその他の必要な措置を講じて伝播を遮断するよう関係機関に通知しなければならない。

第 5 章　监测预警与应急处置

第 5 章　モニタリング事前警告及び緊急対応処置

第 51 条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第 51 条 国は、ネットワークの安全のモニタリング事前警告及び情報通報の制度を確立する。国のネットワーク安全情報化機関は、関係機関を統括してネットワークの安全情報の収集、分析及び通報業務を強化し、規定に従いネットワークの安全のモニタリング事前警告情報を統一的に発表しなければならない。

第 52 条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第 52 条 重要情報インフラストラクチャーの安全保護業務に責任を負う機関は、当該業界及び当該分野のネットワークの安全のモニタリング事前警告及び情報通報制度を確立して健全化し、なお且つ規定に従いネットワークの安全のモニタリング事前

警告情報を送付し報告しなければならない。

第 53 条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第 53 条 国のネットワーク安全情報化機関は、関係機関と連携してネットワークの安全にかかるリスク評価及び緊急対応業務メカニズムを確立して健全化し、ネットワークの安全にかかる事件のための緊急対応マニュアルを制定し、なお且つ訓練を定期的に実施する。

重要情報インフラストラクチャーの安全保護業務に責任を負う機関は、当該業界及び当該分野のネットワークの安全にかかる事件のための緊急対応マニュアルを制定し、なお且つ訓練を定期的に実施しなければならない。

ネットワークの安全にかかる事件のための緊急対応マニュアルについては、事件発生後の危害程度、影響範囲等の要素に従いネットワークの安全にかかる事件についてレベル分けし、なお且つ相応する緊急対応処置措置を定めなければならない。

第 54 条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第 54 条 ネットワークの安全にかかる事件に発生するリスクが増大する際には、省級以上の人民政府の関係機関は、所定の権限及び手続に従い、なお且つネットワークの安全にかかるリスクの特徴及びもたらされるおそれのある危害に基づき、次に掲げる措置を講じなければならない。

(1) 関係機関、組織及び人員に対し、遅滞なく関係情報を収集、報告し、ネットワークの安全にかかるリスクについてのモニタリングを強化するよう要求する。

(2) 関係機関、組織及び専任者を組織し、ネットワークの安全にかかるリスク情報について分析評価を行い、事件発生の可能性、影響範囲及び危害程度を予測する。

(3) 社会に対しネットワークの安全のリスク事前警告を発表し、危害を回避し、軽減するための措置を発表する。

第 55 条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第 55 条 ネットワークの安全にかかる事件が発生した場合には、直ちにネットワークの安全にかかる事件のための緊急対応マニュアルを始動し、ネットワークの安全にかかる事件について調査及び評価をし、ネットワークプロバイダに対し技術措置その他の必要措置を講じ、安全の潜在的危険を消去し、

危害の拡大を防止するよう要求し、なお且つ公衆に関係のある警告情報を遅滞なく社会に対し発表しなければならない。

第 56 条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第 56 条 省級以上の人民政府の関係機関は、ネットワークの安全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安全にかかるリスクが存在するか、安全上の事件が発生したことを発見した場合には、所定の権限及び手続に従い当該ネットワークプロバイダの法定代表者又は主たる責任者に対し行政指導をすることができる。ネットワークプロバイダは、要求に従い措置を講じて是正し、潜在的危険を消除しなければならない。

第 57 条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第 57 条 ネットワークの安全にかかる事件に起因して、突発事件又は生産安全事故が発生した場合には、『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』等の関係する法律及び行政法規の規定により処置しなければならない。

第 58 条 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第 58 条 国の安全及び社会公の秩序の維持・保護並びに重大な突発的社会安全事件の処置にかかる必要に起因し、国務院の決定又は承認を経た場合には、特定区域においてネットワーク通信に対し制限等の臨時措置を講じることができる。

第 6 章　法律责任

第 6 章　法的責任

第 59 条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

第 59 条 ネットワークプロバイダが本法第 21 条又は第 25 条所定のネットワークの安全の保護義務を履行しない場合には、関係所管機関が是正するよう命じ、警告する。是正を拒否するか、ネットワークの安全を脅かす等の結果をもたらした場合には、1 万元以上 10 万元以下の制裁金を科し、直接の責任を負う所管者に対しては5千元以上5万元以下の制裁金を科する。

重要情報インフラストラクチャーの運営者が本法第 33 条、第 34 条、第 36 条又は第 38 条所定のネットワークの安全の保護義務を履行しない場合には、関係所管機関が是正するよう命じ、警告する。是正を拒否するか、ネットワークの安全を脅かす等の結果をもたらした場合には、10 万元以上 100 万元以下の制裁金を科し、直接の責任を負う所管者に対しては1万元以上10万元以下の制裁金を科する。

第 60 条 本法第 22 条第 1 項若しくは第 2 項又は第

第 60 条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

48 条第 1 項の規定に違反し、次に掲げる行為の 1 つをした場合には、関係所管機関が是正するよう命じ、警告する。是正を拒否するか、ネットワークの安全を脅かす等の結果をもたらした場合には、5 万元以上 50 万元以下の制裁金を科し、直接の責任を負う所管者に対しては 1 万元以上 10 万元以下の制裁金を科する。

（一）设置恶意程序的；

(1) 悪意のあるプログラムを設置する行為

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

(2) その製品及びサービスに存在する安全の欠陥、セキュリティホール等のリスクに対し直ちに救済措置を講じない行為か、規定どおりに遅滞なく使用者に対し告知し、なお且つ関係所管機関に対し報告しない行為

（三）擅自终止为其产品、服务提供安全维护的。

(3) その製品及びサービスのため安全の維持・保護を提供することを無断で終了する行為

第 61 条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第 61 条 ネットワークプロバイダが本法第 24 条第 1 項の規定に違反し、使用者に対し真実の身分情報を提供するよう要求しないか、真実の身分情報を提供しない使用者に対し関連サービスを提供した場合には、関係所管機関が是正するよう命ずる。是正を拒否するか、情状が重大であるときは、5 万元以上 50 万元以下の制裁金を科し、なお且つ関係所管機関が関連業務の一時停止、操業停止・整頓、ウェブサイトの閉鎖、行政処分としての関連業務許可証の取消し又は行政処分としての営業許可証の取消しを命じ、直接の責任を負う所管者その他の直接責任者に対しては 1 万元以上 10 万元以下の制裁金を科することができる。

第 62 条 违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

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、検査測定、リスク評価等の活動を展開した場合又は社会に対しシステムのセキュリティホール、コンピューターウィルス、サイバー攻撃、ネットワーク侵入等のネットワークの安全情報を頒布した場合には、関係所管機関が是正するよう命じ、警告をする。是正を拒否するか、情状が重大であるときは、1 万元以上 10 万元以下の制裁金を科するものとし、なお且つ関係所管機関が関連業務の一時停止、業務停止・整頓、ウェブサイトの閉鎖、行政処分としての関連業務許可証の取消し又は行政処分としての営業許可証の取消しを命じ、直接の責任を負う所管者その他の直接責任者に対しては

5千元以上5万元以下の制裁金を科することができる。

第63条 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

第63条 第27条の規定に違反し、ネットワークの安全を脅かす活動に従事した場合か、ネットワークの安全を脅かす活動に専ら使用するプログラム若しくは工具を提供した場合か、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技術サポート、広告普及、支払決済等の援助を提供した場合において、なお犯罪を構成しないときは、公安機関が違法所得を没収し、5日以下の拘留を科するものとし、5万元以上50万元以下の制裁金を併科することができる。情状が比較的重大であるときは、5日以上15日以下の拘留を科するものとし、10万元以上100万元以下の制裁金を併科することができる。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

事業者が前項の行為をした場合には、公安機関が違法所得を没収し、10万元以上100万元以下の制裁金を科し、なお且つ直接の責任を負う所管者その他の直接責任者に対しては前項の規定により処分する。

违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

本法第27条の規定に違反し、治安管理の処分を受けた者は、5年間、ネットワークの安全管理及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。刑事処分を受けた者は、終身においてネットワークの安全管理及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。

第64条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

第64条 ネットワークプロバイダ又はネットワーク製品若しくはサービスの提供者が本法第22条第3項又は第41条から第43条の規定に違反し、個人情報の法により保護を受ける権利を侵害した場合には、関係する所管機関が是正するよう命ずるものとし、情状に基づき警告、違法所得の没収又は違法所得の相当額以上10倍以下の制裁金を単科するか、併科することができる。違法所得がないときは、100万元以下の制裁金を科し、直接の責任を負う所管者その他の直接責任者に対しては1万元以上10万元以下の制裁金を科する。情状が重大である場合には、関連業務の一時停止、操業停止・整頓、ウェブサイトの閉鎖、行政処分としての関連業務許可証の取消し又は行政処分としての営業許可証の取消しを命ずることができる。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所

本法第44条の規定に違反し、個人情報を窃取するか、その他の不法な方式により取得し、違法に販売するか、不法に他人に対し提供した場合で、犯罪

得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

を構成しないとき、公安機関が違法所得を没収し、なお且つ違法所得の相当額以上 10 倍以下の制裁金を併科し、違法所得がない場合には、100 万元以下の制裁金を科する。

第 65 条 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第 65 条　重要情報インフラストラクチャーの運営者が本法第 35 条の規定に違反し、安全審査を経ていないか、安全審査に合格していないネットワーク製品又はサービスを使用した場合には、関係所管機関が使用を停止するよう命じ、調達金額の相当額以上 10 倍以下の制裁金を科する。直接の責任を負う所管者その他の直接責任者に対しては、1 万元以上 10 万元以下の制裁金を科する。

第 66 条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第 66 条　重要情報インフラストラクチャーの運営者が本法第 37 条の規定に違反し、国外にネットワークデータを保存するか、国外に対しネットワークデータを提供した場合には、関係所管機関が是正するよう命じ、警告をし、違法所得を没収し、5 万元以上 50 万元以下の制裁金を科するものとし、なお且つ関連業務の一時停止、操業停止・整頓、ウェブサイトの閉鎖、行政処分としての関連業務許可証の取消し又は行政処分としての営業許可証の取消しを命ずることができる。直接の責任を負う所管者その他の直接責任者に対しては 1 万元以上 10 万元以下の制裁金を科する。

第 67 条 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

第 67 条　本法第 46 条の規定に違反し、違法な犯罪行為の実施に使用するウェブサイト及び通信グループを設立するか、ネットワークを利用して違法な犯罪行為の実施に関わる情報を頒布した場合において、なお犯罪を構成しないときは、公安機関が 5 日以下の拘留を科するものとし、1 万元以上 10 万元以下の制裁金を併科することができる。情状が重大である場合には、5 日以上 15 日以下の拘留を科するるものとし、5 万元以上 50 万元以下の制裁金を併科することができる。違法な犯罪行為の実施に用いたウェブサイト及び通信グループは、これらを閉鎖する。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

事業者が前項の行為をした場合には、公安機関が 10 万元以上 50 万元以下の制裁金を科し、なお且つ直接の責任を負う所管者その他の直接責任者に対しては前項の規定により処分する。

第 68 条 网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、

第 68 条 ネットワークプロバイダ本法第 47 条の規定に違反し、法律及び行政法規により頒布又は伝送

采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

が禁止される情報につき伝送を停止せず、消去等の処置措置を講じないか、関係記録を保存しない場合は、関係する所管機関が是正するよう命じ、警告を行い、違法所得を没収する。是正を拒否するか、情状が重大であるときは、10 万元以上 50 万元以下の制裁金を科するものとし、なお且つ関連業務の一時停止、操業停止・整頓、ウェブサイトの閉鎖、行政処分としての関連業務許可証の取消し又は行政処分としての営業許可証の取消しを命ずることができる。直接の責任を負う所管者その他の直接責任者に対しては 1 万元以上 10 万元以下の制裁金を科する。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

電子情報発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 48 条第 2 項所定の安全管理義務を履行しない場合には、前項の規定により処分する。

第 69 条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

第 69 条 ネットワークプロバイダが本法の規定に違反し、次に掲げる行為の一つを犯した場合には、関係所管機関が是正するよう命ずる。是正を拒否するか、情状が重大であるときは、5 万元以上 50 万元以下の制裁金を科するものとし、直接の責任を負う所管者その他の直接責任者に対しては、1 万元以上 10 万元以下の制裁金を科する。

（一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；

(1) 関係機関の要求どおりに法律及び行政法規により頒布又は伝送が禁止される情報について、伝送停止、消去等の処置措置を講じなかったとき。

（二）拒绝、阻碍有关部门依法实施的监督检查的；

(2) 関係機関が法により実施する監督検査を拒否するか、妨害したとき。

（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

(3) 公安機関及び国家安全機関に対し技術サポート及び援助の提供を拒否したとき。

第 70 条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

第 70 条 本法第 12 条第 2 項並びにその他の法律及び行政法規により頒布又は伝送が禁止される情報を頒布するか、伝送した場合には、関係する法律及び行政法規の規定により処分する。

第 71 条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第 71 条 本法所定の違法行為をした場合には、関係する法律及び行政法規の規定により信用ファイルに記入し、なお且つ公示を行う。

第 72 条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关

第 72 条 国家機関政務ネットワークプロバイダが本法所定のネットワークの安全保護義務を履行し

责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

ない場合には、その上級機関又は関係機関が是正するよう命ずる。直接の責任を負う所管者その他の直接責任者に対しては、法により処分する。

第 73 条 网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。

第 73 条 ネットワーク安全情報化機関及び関係機関が第 30 条の規定に違反し、ネットワークの安全保護の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た場合には、直接の責任を負う所管者その他の直接責任者について、法により処分する。

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

ネットワーク安全情報化機関及び関係機関の職員が職務を懈怠し、職権を濫用するか、私利をはかった場合において、なお犯罪を構成しないときは、法により処分する。

第 74 条 违反本法规定，给他人造成损害的，依法承担民事责任。
违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第 74 条 本法の規定に違反し、他人に損害をもたらした場合には、法により民事責任を負う。
本法の規定に違反し、治安管理違反行為を構成する場合には、法により治安管理にかかる処分を行う。犯罪を構成する場合には、法により刑事責任を追及する。

第 75 条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第 75 条 国外の機関、組織及び個人が攻撃、侵入、妨害、破壊等の中華人民共和国の重要情報インフラストラクチャーを脅かす活動に従事し、重大な結果をもたらした場合、法により法的責任を追及する。また、国務院の公安機関及び関係機関は、当該機関、組織及び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。

第 7 章　附则

第 7 章　附則

第 76 条 本法下列用语的含义：

第 76 条 本法の次に掲げる用語の意義は、当該各号に定めるところによる。

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

(1) 「ネットワーク」とは、コンピュータその他の情報端末及び関連設備により構成され、一定の規則及びプログラムに従い情報について収集、保存、伝送、交換及び処理をするシステムをいう。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

(2) 「ネットワークの安全」とは、必要な措置を講じることを通じて、ネットワークに対する攻撃、侵入、妨害、破壊及び不法使用並びに突発的事故を防止し、ネットワークが安定かつ信頼可能な運行状態にあるようにし、並びにネットワークデータの完全性、秘密保持性及びユーザビリティを保障する能力

をいう。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

(3) 「ネットワークプロバイダ」とは、ネットワークの所有者及び管理者並びにネットワークサービスの提供者をいう。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

(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、処理され、及び生じた各種電子データをいう。

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

(5) 「個人情報」とは、電子データその他の方式により記録され、単独又はその他の情報と組み合わせて自然人の個人身分を識別することができる各種情報をいう。これには、自然人の氏名、生年月日、身分証番号、個人の生物識別情報、住所、電話番号等を含むが、これらに限らない。

第 77 条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第 77 条 国家秘密に関わる情報の保存及び処理にかかるネットワークの運行の安全保護については、本法を遵守するべきほか、更に秘密保持にかかる法律及び行政法規の規定を遵守しなければならない。

第 78 条 军事网络的安全保护，由中央军事委员会另行规定。

第 78 条 軍事に関わるネットワークの安全の保護については、中央軍事委員会が、これを別途定める。

第 79 条 本法自 2017 年 6 月 1 日起施行。

第 79 条 本法は、2017 年 6 月 1 日から施行する。