資料解題

中華人民共和国サイバーセキュリティー法

山 本　賢 二*

「中華人民共和国サイバーセキュリティー法」（中华人民共和国网络安全法・Cybersecurity Law of the People's Republic of China）は第12期全人代常務委員会第15回会議の審議を経て2015年7月6日に草案が公表され、「中国人代網」（中国人大网）を通じて8月5日まで意見を募った後、第12期全人代常務委員会第21回会議によって審議、2016年7月5日に第2次草案（草案二次审议稿）が公表され、8月4日まで再び意見を募った後、全国人民代表大会常務委員会第24回会議によって審議、賛成154票、棄権1票で可決採択され、2016年11月7日に公布、2017年6月1日に施行された。

同法の採択を報じる2016年11月7日の新華社電はリードの部分で「これはわが国のネットワーク領域における基礎的法律であり、明確に個人情報に対する保護を強化し、ネットワーク詐欺に打撃を与えるものである。」（这是我国网络领域的基础性法律，明确加强对个人信息保护，打击网络诈骗。）と伝えている。

1．「サイバー法」に対する所感

筆者は本誌10号（2017.3）の「海外研究動向　中国」「習近平執政4年と中国の言論空間」（pp.269-289）の中で、筆者自身の関心の所在から同法の内容について触れている。

もとより、筆者は2009年7月5日、新疆ウイグル自治区の区都ウルムチ市で発生した民族衝突事件（「7.5」事件）後に行われたネットワーク遮断という超法規的措置が同法にどのような条文になって明記されるのかに最大の関心があったため、関連条文を冒頭に取り上げるとともに、いくつかのカテゴリーに分けて所感を述べた。昨年の同文では「インターネット安全法」とし、略称も「ネット法」として論じていたが、「网络安全」という中国語に「サイバーセキュリティー」という定訳があることと同法の英訳が「Cybersecurity Law of the People's Republic of China」となっていることから、本稿では「サイバーセキュリティー法」とし、それに基づき下記の再録では文言を一部修正している。

（再録）

第58条　国家の安全と社会の公共秩序を守ることで、重大な突発社会安全事件を処理する必要から、国務院の決定、あるいは承認を経て、特定区域においてネットワーク通信に対し制限などの臨時措置を講ずることができる。

*やまもと　けんじ　日本大学法学部新聞学科　教授

（原文）
第五十八条　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。

「草案」には「第 50 条　国家の安全と社会の公共秩序を守ることで、重大な突発社会安全事件を処理する必要から、国務院、あるいは省、自治区、直轄市人民政府は国務院の承認を経て、一部地域においてネットワーク通信に対し制限などの臨時措置を講ずることができる。」（原文：第五十条　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，国务院或者省、自治区、直辖市人民政府经国务院批准，可以在部分地区对网络通信采取限制等临时措施。）とあり、「省、自治区、直轄市人民政府」もネット遮断の権限をもつ内容であったが、この部分は二次草案の第 56 条で削除され、そのまま「サイバーセキュリティー法」の第 58 条に引き継がれた。すなわち、「サイバーセキュリティー法」ではネット遮断の権限は中央政府のみがもつものであって、地方政府にはその権限がないことを明記したのである。

⑴　適用範囲

第 2 条　中華人民共和国域内でのネットワーク建設、運営、維持と使用、およびサイバーセキュリティーの監督管理には本法が適用される。

（原文）
第二条　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。

「サイバーセキュリティー法」は「第 2 条」にその適用範囲を上記のように明記している。これは「草案」、「二次草案」いずれも「第 2 条」に置かれ、同じ内容である。ここで言うところの「中華人民共和国域内」には香港、マカオという二つの特別行政区が含まれるのか、他の条文を含めて明確にされていない。

⑵　管理責任

第 8 条　国家ネットワーク情報部門はサイバーセキュリティー工作と関係監督管理工作を統括調整する責任を負う。国務院電信主管部門、公安部門とその他の関係機関は本法と関係法律、行政法規の規定に合わせて、各自の職責の範囲内でサイバーセキュリティーの保護と監督管理工作の責任を負う。県級以上の地方人民政府の関係部門のサイバーセキュリティーの保護と監督管理の職責は、国家の関係規定に合わせて確定する。

（原文）
第八条　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。

ここでは中央においては「国家ネットワーク情報部門」と「国務院電信主管部門、公安部門とその他の関係機関」、地方においては「県級以上の地方人民政府の関係部門」によってネットが管理されることが明文化されている。

この条文は「草案」では「国務院電信主管部門、公安部門とその他の関係機関」との文言が「・・・国務院工業・情報化、公安部門とその他の関係部門・・・」（原文：国务院工业和信息化，公安部门和其他有关部门）となっていたところ、「二次草案」で修正されすでにこの内容になっていた。

⑶　禁止事項

第 12 条　国家は公民、法人とその他の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し、ネットワークサービスのレベルを向上させ、社会に安全、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律に基づく秩序ある自由な流通を保障する。

如何なる個人や組織もネットワーク使用には、憲法法律を遵守、公共秩序を遵守、社会公徳を尊重しなければならず、サイバーセキュリティーに危害を及ぼしてはならず、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及ぼし、国家政権転覆、社会主義制度ひっくり返すことを煽動し、国家分離、国家統一破壊を煽動、テロリズム、過激主義を宣揚、民族怨恨、民族蔑視を宣揚、暴力、猥褻色情情報を伝播、虚偽情報をねつ造、伝播させ経済秩序と社会秩序を混乱させたり、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。

（原文）
第十二条　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。

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。

「サイバー法」は上掲のように「第 12 条」で「ネットワーク情報の法律に基づく秩序ある自由な流通を保障する。」としたうえで、「禁止事項」を規定している。ネットワークを通じて流してはいけない情報を箇条書きにすると次の 12 項目になる。

①　憲法法律を遵守しないもの

② 公共秩序を遵守しないもの
③ 社会公徳を尊重しないもの
④ サイバーセキュリティーに危害を及ぼすもの
⑤ 国家の安全、栄誉と利益に危害を及ぼすもの
⑥ 国家政権転覆、社会主義制度ひっくり返すことを煽動するもの
⑦ 国家分離、国家統一破壊を煽動するもの
⑧ テロリズム、過激主義を宣揚するもの
⑨ 民族怨恨、民族蔑視を宣揚するもの
⑩ 暴力、猥褻色情情報を伝播するもの
⑪ 虚偽情報をねつ造、伝播させ経済秩序と社会秩序を混乱させるもの
⑫ 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もの

冒頭の3行（日訳）は「草案」（第9条）、「二次草案」（第12条）を通じて変わっていない。

その下の文言については「草案」に無い文言は、「・・・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及ぼし、国家政権転覆、社会主義制度ひっくり返すことを煽動し、国家分離、国家統一破壊を煽動、テロリズム、過激主義を宣揚、民族怨恨、民族蔑視を宣揚、暴力、猥褻色情情報を伝播、虚偽情報をねつ造、伝播させ経済秩序と社会秩序を混乱させたり、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。」の中の「栄誉と利益」、「国家政権転覆、社会主義制度をひっくり返すことを煽動し、国家分離、国家統一破壊を煽動」、「虚偽情報をねつ造、伝播させ経済秩序」、「名誉、プライバシー、知的財産権」などであり、これらは「二次草案」で加えられていた。ここから採択された「サイバー法」の条文が禁止事項についてより詳細に規定していることが分かる。

⑷ 実名制

第24条　ネットワーク運営者はユーザーのためにネットワーク接続、アカウント名登録を処理、固定電話、移動電話のネットワーク加入手続きを処理したり、あるいはユーザーのために情報配信、インスタントメッセジャーなどのサービスを提供する上で、ユーザーと取り決めに調印、あるいは提供するサービスを確認するとき、ユーザーに真実の身分情報の提供を要求すべきである。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それに関係サービスを提供することができない。

国家はネットワーク身分信頼戦略を実施し、安全、便利な電子身分認証技術研究開発を支持し、異なる電子身分認証間の相互認証を推進する。

（原文）
第二十四条　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。

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。

この「二次草案」（23 条）と同じ内容である条文は「真実の身分情報」（実名）を提供しないものはネットワークを利用できないことを明文規定したものである。この条文の「草案」に無く、「二次草案」から加えられた文言は「・・・为用户提供信息发布、即时通讯等服务，・・・」の「インスタントメッセジャーなど」（「即时通讯等」）と「・・・应当要求用户提供真实身份信息。」の「すべきである」（「・・・应当」）、「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，」の「ネットワーク身分信頼戦略を実施し」（「・・・实施网络可信身份战略・・・」）であり、「草案」から削除されたのは「・・・推动不同电子身份认证之间的互认。」の後にあった「通用」である。

⑸　捜査協力

第 28 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いて国家安全を守り、犯罪を捜査する活動に技術的支援と協力を提供すべきである。

（原文）
第二十八条　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。

この条文も「二次草案」を踏襲したものである。この条文になる前の「草案」は「第 23 条」で「国家の安全と犯罪捜査の必要から、捜査機関は法律の規定に合わせて、ネットワーク運営者に必要な支援と協力を要求することができる。」（原文：第二十三条　为国家安全和侦查犯罪的需要，侦查机关依照法律规定，可以要求网络运营者提供必要的支持与协助。）としていた。「サイバー法」は「ネットワーク運営者」の捜査協力への義務化を明確にしたものと言える。

もとより、習近平は 2015 年 12 月 16 日から 18 日にかけて開催された中国主催の第二回世界インターネット大会で講話を行い、「四つの原則」を提示、そのトップに「ネット主権の尊重」（尊重网络主权）を挙げ、「『国連憲章』の確立した主権平等の原則は現代の国際関係の基本的準則であり、国と国の往来する諸領域をカバーするものであり、その原則と精神はネット空間にも適用されるべきである。」（新華社 2015 年 12 月 16 日電）と語っている。「サイバー法」がこの「ネット主権」論を基礎に制定されたことは疑いのないところである。すなわち、この「サイバー法」の制定は習の下で「国家主権」→「情報主権」→「ネット主権」という構図の中に中華人民共和国の情報管理政策が立案されていることの一つの反映でもある。

以上再録したのは、筆者の関心のあるところ、すなわち中国のメディア・ジャーナリズム、特に「言論の自由」に係わる条文であったが、同法の内容について、強く反応したのは日本を含む在華

企業を擁する世界の産業界であった。

2．外国経済団体などの書簡

この「サイバー法」が可決されると、11 月 11 日、米国情報技術工業協議会　インターネット協会、米商工会議所、豪経済団体ＡＩＧ、ビジネスヨーロッパなど世界各国 40 を超える経済団体、技術関連団体が連名で下掲の書簡を中国の習近平総書記が自ら「グループ長」を兼務している「中国共産党中央サイバーセキュリティー・情報化指導小グループ」（中国共产党中央网络安全和信息化领导小组）宛に送った。日本では JEITA，JBMIA，CIAJ，JISA，経団連，日本商工会議所，中国日本商会の各団体が署名している。

2016 年 11 月 11 日
致：中国共产党中央网络安全和信息化领导小组
抄送：中央网络安全和信息化领导小组办公室
北京东城区朝阳门内大街 225 号，100010
中华人民共和国商务部
北京东长安街 2 号 100731

尊敬的中央网络安全和信息化领导小组：

我们代表了广泛分布于各行各业的公司，与中国有着深厚且长期的商业联系。我们赞赏中国政府在制定网络安全法的过程中曾表示理解国际上包括保险业和其他行业组织在内的各行业组织对中国网络安全法草案及网络安全相关规定和措施的关切。我们在 2016 年 8 月 10 日致李克强总理的信中也再次表达了我们的关切。但在刚刚通过的网络安全法的正式文本中，我们发现国际工商界高度关切的一些实质性问题仍未得到解决。对此我们感到失望。

长期以来，我们的会员公司坚定致力于与中国政府合作，共同寻求在支持实现安全、经济与社会目标的前提下，同时解决国际产业界合理担忧的行之有效解决方案。然而，眼下让我们深以为忧的是，当前正在讨论之关于安全方面的规定，很可能造成国与国之间的贸易壁垒，不仅不能实现其合理的安全目标（甚至降低其安全性），还给产业界增加沉重的负担，损害了中国与其贸易伙伴国之间的良好关系。让我们忧虑的是，中国在网络安全方面采取的措施将严重阻碍、而非促进中国进一步融入全球经济体系的步伐。此外，在当今全球政治与社会发生重大变革的时代，制定这类政策规定将加剧当今全球市场令人不安的趋势，与开拓贸易合作及国际化背道而驰。

我们一直且依然期盼中国政府最高决策层能够采取切实有效的措施，履行以往的承诺，与其他国家共同推行制定鼓励竞争且非歧视的信息通信技术安全政策。这些承诺包括，所制定 ICT 政策措施应对工商界在采购、销售、和使用 ICT 产品的各个环节具有广泛的适用性，并考虑国际通行规范，对国内外产品一视同仁，不对技术产品施加不必要地国别的条件或限制。

我们认为，对于这些正在讨论中的网络安全规定，包括要求保险业、金融业和其它行业采用安全可控技术的相关规定与即将实施的网络安全法规定和标准在内，应当遵守中国加入世界贸易组织（WTO）的承诺，鼓励采用国际通行模式，以便中国发展成为全球技术与服务中心。我们关切的是，中国提出了针对信息技术产品和服务的自主可控产品替代计划，违反了中国的入世承诺。我们尤其对新网络安全法中的一些规定及相关措施深为担忧，如规定数据境内存储和处理，限制跨境数据流动，对信息化

产品和服务开展安全审查及相关要求，这阻碍了贸易的进行，此外对数据共享及提供技术协助也做出了广泛的规定，极可能削弱产品的安全性并损害了消费者的隐私保护。我们各协会在此前提交给中国政府的意见函和其他材料中已对我们关切的这些问题做了详细阐述，详见如下材料。

我们以上关切的事项涉及对中国经济影响深远的问题，中国与商贸伙伴国的关系，以及全球经济。我们意识到，各国监管机构在管理新技术以及解决安全问题方面都面临着巨大的挑战。但我们诚恳地希望中国的网络安全政策能够更好地反映信息通信行业的全球性本质，促进市场竞争，提高透明度，允许各商业企业采购设备与软件时，能够自主地确定技术要求。据我方会员公司的共同经验，坚持上述原则的国家，其技术行业的竞争力和安全性往往更具优势。

感谢中央网络安全和信息化领导小组考虑我们的意见。我们希望能够与领导小组成员单位及相关领导就我们关切的问题作进一步探讨，届时我们将就我方所关切的问题提供相关的说明和详细资料。本函随附一套汇总的意见函，以便更全面、详细地说明我们对上述关切的思考关切，谨供参考。

顺致敬意

上掲の書簡は概ね次のように指摘している。

セキュリティ分野の規定は国と国との貿易障壁を作る可能性があり、中国がサイバーセキュリティー分野で採る措置は中国がさらにグローバル経済に溶け込む歩みを促進するのではなく、大いに阻害する。それはグローバル市場における懸念の趨勢を加速し、貿易協力及び国際化とは逆の方向に進む。金融やその他の業種が採用すべきとするセキュリティ技術に関する規定は、中国がWTO に加盟した際のコミットメントを遵守すべきであり、国際的に通用しているモデルの採用を奨励すべきである。

中国は情報技術製品とサービスに関連し、自国でコントロールできる製品に変える計画を提起しているが、中国の WTO 加盟時のコミットメントに背いている。特に関心をもつのが、データの域内での保存と処理、国境を越えての情報の流通制限、情報関連製品とサービスにたいする安全審査御呼び関係要求などであり、それは貿易の進展を阻害する。このほか、データの共有、技術協力にも幅広い規定があるが、製品の安全性を弱体化するとともに消費者のプライバシーの保護を損なう可能性が極めて高い。

3．日本中国商会など 4 団体の 2 次草案に対する意見書

これより先、中国日本商会は「サイバー法」の 2 次草案についての意見募集が行われたことを受け、「日本电子信息技术产业协会（JEITA）、日本信息通信网络产业协会（CIAJ）、日本办公机械与信息系统产业协会（JBMIA）」とともに 2016 年 8 月 4 日付で全国人大常委会法制工作委员会に対して意見書（http://cjcci.org/uploads/mail_attachment/1473066578.docx）を提出している。この 18 項目の意見と、3 項目の質問からなる意見書は冒頭次のように指摘している。

「一次草案に対する意見の中で、以下の 3 点の内容を指摘したが、今回の二次草案に対しても同様に、依然としてわれわれは憂慮している。」（在针对一次草案的意见中，我们指出了以下 3 点内容，此次对于二次草案，我们依然抱有同样的担忧。）とし、その 3 点を「国を越えての情報の自由な伝播を不必要に制限することはインターネット社会の発展を阻害し、外国企業の市場参入を阻害

するものであり、過度の制限といえる。」（我们认为，不必要地限制跨国信息的自由传播，将妨碍互联网社会的发展，阻碍外国企业进入市场，属于过度限制。）、「サイバー空間の中のリスクは国の境を越えてのグローバルの問題であり、サイバーセキュリティ―の措置に確実に効果のあがる役割を真に発揮させるには、グローバルな解決方法が必要であり、中国が特有の国家標準を採用する方法は恐らくセキュリティ―の保障を強化する目的とは逆の方向に向かうことになる。」（我们认为网络空间中的风险是超越国界的全球性问题，网络安全措施要真正发挥切实有效的作用，需要全球性的解决方案，而中国采用特有的国家标准的做法恐怕与加强安全保障的目的背道而驰。）、「本法の適用範囲は一次草案に比べさらに抽象的になっている。このほか、一部の条文の具体的要求が不明確であり、現在あるセキュリティー制度との間の関係が不明確であり、本法に基づくと、どの領域がどのような制限を受けるのか予測し難いと同時に、今後法律執行の透明性を確保するのが難しいことが懸念される。」（本法的适用范围较一次草案更加抽象。另外，部分条文的具体要求不明确，与现存安全制度之间的关系亦不明确，难以预测根据本法哪些领域将受到哪些限制，同时，也令人担忧今后难以确保法律执行的透明性。）、「ICT 領域の技術革新を推進し、同時に効果的にセキュリティーの脅威を制御するためには、制度設計プロセスの高度な透明性を確保し、市場の開放を維持し、合理的かつ実効のあがるセキュリティー保障措置を採らなければならない。われわれは中国に、WTO の加盟国として、国際間の約束を遵守し、より一層不必要な貿易制限措置を減らし、国内外の企業に平等に開放される市場を造り、一つの揺るぎない、弾力性に富んだ、ICT ネットワーク社会建設を目指してもらいたいと切に願っている。」（为了推进 ICT 领域的技术革新，同时有效抵御安全威胁，必须确保制度设计程序的高度透明，保持市场开放，采取合理而切实有效的安全保障措施。我们衷心希望中国作为 WTO 成员国，能够遵守国际约定，进一步减少不必要的贸易限制措施，打造面向国内外企业平等开放的市场，力争建设起一个坚不可摧、富有弹性的 ICT 网络社会。）

同「意見書」は以上のような総体的な懸念に基づいて、具体的な意見を述べている。その中で挙げられた条文は以下の通り。

第 14 条

第十四条　国家は、サイバーセキュリティー標準体系を確立し、整備する。国務院標準化行政主管部門と国務院のその他の関係部門は、それぞれの職責に基づいて、サイバーセキュリティー管理及びネットワーク製品、サービスと運用安全に関係する国家標準、業種標準を組織制定する。

国家は、企業、ネットワーク関連の業種組織などがサイバーセキュリティー国家標準、業種標準の制定に参与することをサポートするとともに、企業が国家標準、業種標準に厳しい企業標準を制定することを奨励する。

（原文）

第十四条　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、网络相关行业组织等参与网络安全国家标准、行业标准的制定，并鼓励企业制定严于国家标准、行业标准的企业标准。

第 21 条
第二十一条　ネットワーク製品、サービスは関係する国家標準の強制的要求と合致させるべきである。ネットワーク製品、サービスの提供者は悪意のあるプログラムを設置してはならない。そのネットワーク製品、サービスに安全上の欠陥、不備などのリスクがあることを発見したら、すぐに補完措置を講じて、規定に従って適時にユーザーに告示すると共に、関係主管部門に報告すべきである。
　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、引き続き安全維持の提供をすべきであり、規定または当事者の取り決めの期限内に、安全維持の提供を終了してはならない。
　ネットワーク製品、サービスにユーザー情報の収集機能がある場合、その提供者はユーザーに明示する共に、同意を得るべきである。ユーザーの個人情報にかかわる場合、さらに、本法と関連の法律、行政法規の個人情報に関する規定も遵守すべきである。
（原文）
第二十一条　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，应当及时告知用户并采取补救措施，并按照规定向有关主管部门报告。
　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间内，不得终止提供安全维护。
　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；收集公民个人信息的，应当遵守本法和有关法律、行政法规关于公民个人信息保护的规定。

第 22 条
第二十二条　ネットワークの基幹設備とサイバーセキュリティーの専用製品は関係する国家の標準の強制的要求に合わせるべきであり、資格を備える機関によって安全認証に合格した、または安全検査測定の要求と合致した後、はじめて販売できる。国家ネットワーク情報部門は国務院の関係部門と共にネットワークの基幹設備とサイバーセキュリティーの専用製品のカタログを作り、公布するとともに、安全認証と安全検査測定の結果の相互認証を推進して、認証、検査測定の重複を回避させる。
（原文）
第二十二条　网络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。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。

第 27 条
第二十七条　ネットワーク運営者は公安機関、国家安全機関の法に基づき国家安全を守ることと犯罪事件を捜査する活動のために、技術的サポートと協力を提供すべきである。
（原文）
第二十七条　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 29 条
第二十九条　国家は、一旦破壊され、機能を失ったか、またはデータの漏洩によって、国家の安全、国民の経済と人民生活、公共の利益に重大な脅威を与える可能性のある基幹情報インフラに対し、サイバーセキュリティー等級保護制度を基礎にして、重点的保護を実行する。基幹情報インフラの安全保護の具体的範囲と安全保護の弁法は国務院によって制定される。
　国家は、基幹情報インフラ以外のネットワーク運営事業者が自発的に基幹情報インフラ保護体系に参与するよう奨励する。
（原文）
第二十九条　国家对一旦遭到破坏、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。
　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。

第 33 条
第三十三条　基幹情報インフラの運営者はネットワークの製品購入またはサービスをするのに、国家安全に影響を与える可能性がある場合は、国家のネットワーク情報部門が国務院の関連部門と組織した安全審査を通すべきである。
（原文）
第三十三条　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会同国务院有关部门组织的国家安全审查。

第 35 条
第三十五条　基幹情報インフラの運営者は中華人民共和国域内で運営中に収集、生まれた公民の個人情報と重要なデータを域内に保存すべきである。業務の需要のため、確かに域外に提供する必要がある場合は、国家のネットワーク情報部門が国務院の関連部門と共に制定した弁法に合わせて安全評価を行うべきである。法律、行政法規に別に規定がある場合は、その規定に従う。
（原文）
第三十五条　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公民个人信息和重要业务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 46 条
第四十六条　いかなる個人や組織から配信された電子情報、提供された応用ソフトも悪意あるプログラムを設定してはならず、法律、行政法規により公表、伝送の禁止されている情報を含んではならない。
　電子情報の配信サービス提供者と応用ソフトのダウンロードサービス提供者は安全管理の義務を

履行すべきであり、そのユーザーに前款の規定に違反する行為があることを知ったら、サービスの提供を停止すべきであり、削除など措置を講じ、関係記録を保存すると共に関係主管部門に報告すべきである。
（原文）
第四十六条　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。
　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，发现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，并向有关主管部门报告。

第 67 条
第六十七条　本法第十二条第二款及びその他の法律、行政法規が公表または伝送を禁止した情報を公表、伝送した場合、関係法律、行政法規の規定に合わせて処罰する。
（原文）
第六十七条　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 56 条
第五十六条　国家安全と社会の公共秩序を守り、重大な突発社会安全事件を処置する必要のため、国務院の決定または承認を経て、特定区域においてネットワーク通信に対して制限など臨時の措置を講じることができる。
（原文）
第五十六条　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 72 条
第七十二条　本法における下記の用語の意味：
（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及び関連の設備によって組成され、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。
（二）　サイバーセキュリティーとは、必要な措置を講じることを通じて、ネットワークに対しての攻撃、侵入、妨害、破壊や不法使用及び意外な事故を防止し、ネットワークを安定・信頼ある運行状態にさせると共に、ネットワークデータの整合性、機密性、利用可能性の能力を保障することを指す。
（三）　ネットワーク運営者とは、ネットワークの所有者、管理者及びネットワークサービス提供者を指す。
（四）　ネットワークデータとは、ネットワークを通じ収集、保存、伝送、処理及び生産する各種の電子データを指す。
（五）　個人情報とは、電子またはその他の方式により記録された単独またはその他の情報と合わ

せて、自然人の個人の身分情報が識別できる各種の情報を指す、しかし、自然人の氏名、生年月日、身分証明書の番号、個人生体識別情報、住所、電話番号などを含むがそれだけに限られない。（原文）

第七十二条　本法下列用语的含义：

（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。

（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。

（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。

（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。

（五）公民个人信息，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公民个人身份的各种信息，包括但不限于公民的姓名、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。

以上の二次草案の条文は後掲する成案（条数は異なるが）とほぼ同じであり、「意見書」の提起した3点をめぐる問題点は解決されるものではなかった。

それがため、前述した世界各国40を超える経済団体、技術関連団体連名の書簡にもこの「意見書」を出したJEITA，JBMIA，CIAJ，中国日本商会の四団体が署名したのである。

4．メディアの反応

この「サイバー法」の施行に当たって、読売新聞は2017年6月5日付の「中国ネット新法　言論統制は正当化できない」と題する社説の中で、「法律には曖昧な規定が多く、中国当局の裁量の余地が大きい。「国家の安全」を名目に、恣意（しい）的に運用し、政府に批判的な言論を封じ込める狙いは明白である。」、「心配されるのは、中国で活動する日本などの外国企業に悪影響を与える規定があることだ。ネットの運営業者や接続業者に対し、個人情報や「重要なデータ」を中国国内のサーバーに保存することを義務付けた。大容量のデータなどを海外に送信する場合は、当局が事前審査するという。機密情報が流出したり、外国企業が中国から本社へ情報を送れなくなったりする恐れがある。中国のネット市場は、利用者が7億人超と急成長している。各国政府や業界団体が、「外国企業を締め出す貿易障壁だ」と、懸念を示したのは当然である。」、「国際基準とかけ離れた「法治」を、外国企業などにも適用する独善的な対応は容認できない。」と批判し、「ネットの利点は、国境がなく、世界の人々を自由につなげることだ。自国に有利な囲い込みはあり得ない。中国は海洋や宇宙でも、一方的な進出や開発で、他国との摩擦を起こしている。責任ある大国の振る舞いではない。」としている。

また、朝日新聞も6月24日付社説「中国ネット法　言論封じる異常な統制」の中で、「今回の法律は利用者の実名登録を徹底させ、ネットを通じた「政権転覆」や「国の分裂」の扇動を禁じる規定を掲げる。ネット空間を厳格に監視する体制を築こうとしている。各国で政府機関や企業がサイバー攻撃にさらされたり、ネット犯罪が横行したりしており、対策は追いついていない。だがそうした問題への取り組みと、言論の封じ込めを混同するわけにはいかない。」、「ネット関連の製品・

サービスは「国家標準に適合しなければならない」とされ、外国企業の事業を制限しかねない。犯罪捜査に際し「技術的支援、協力」を義務づける点については、企業秘密の技術を取られるのではないかと心配されている。データの国外持ち出しに規制をかけているのも穏当ではない。」と批判し、「世界で重きをなし、積極的な外交に打って出る大国が、いっぽうで国を閉ざし、社会を息苦しいものにしている。恣意（しい）的な法執行を少しでもなくすよう、中国の外からも引き続き監視しなければならない。それは声を上げられない中国の市民のためでもある。」としている。」。

その後、ロイターが2017年9月26日、米国が中国にサイバーセキュリティー法の完全施行中止を要求しているとして、次のようなニースを打電した。

［ジュネーブ　26日　ロイター］―米国が中国に対し、同国のサイバーセキュリティー法は世界的な情報のやりとりを阻害するとして、世界貿易機関（ＷＴＯ）サービス貿易理事会での完全施行中止に向けた議論を求めていることが分かった。ＷＴＯが26日、米国が提出した書簡を公表した。

中国は、長年の議論の末に同法を6月に一部施行。国内外の企業に、セキュリティー検査を受けることや、顧客データを中国内に保存することを義務付けた。

米国の書簡は、同法が予定通り2018年末までに現在の形で完全施行されれば、国境を越えたサービスのやりとりが打撃を受ける恐れがあるとしている。書簡は「米国はこれらの懸念について、中国の高官や担当当局に直接伝えてきた」とした上で「中国に対し、懸念が解消されるまでは完全施行を控えるよう求める」としている。

5．習近平のインターネット観

この「サイバー法」は習近平政権の情報管理強化の根幹となる法的根拠を提供するものであるので、国内に対しては厳格に運用されることは疑いのないところである。そこには習近平のインターネットに対する強い警戒心が背景にあるからでもある。

筆者は以前から、2013年8月19、20日の両日北京で開催された全国宣伝思想工作会議の初日の19日に習近平が行った「重要講話」（「8.19講話」）に触れて来た。この会議の開催を伝えた新華社電は習の「8.19講話」の一部のみ伝えただけで、その後も本稿執筆時2017年12月現在、全文は公表されていない。特に、インターネットに関連する部分は新華社電には全くなかった。しかし、ネット上に流布されていた「『8.19』講話精神伝達提綱」（「“8·19”讲话精神传达提纲」）ではインターネットについて習が語っている箇所が少なからぬあった。わけても「輿論闘争の主戦場」という表現は「8.19講話」学習キャンペーンの中にも現れたりしていたこと、さらに2014年5月28日に中央文献出版社から出版された『习近平关于全面深化改革论述摘编』（中共中央文献研究室编辑）の中に習近平の「8.19講話」のインターネット言及部分が初めて公表されたが、その内容が「提綱」と一致していることなどから党内に流された内部文書であることにほぼ間違いがないと筆者は考えている。その内容は習近平執政5年の間に作られたインターネットに関係する法規や動向、特にこの「サイバー法」を読み解くうえで参考にする価値が高いので、下記に再録する。

・・・・・・・・・・

思い切って力を入れ、思い切って管理し、剣を光らせるのに勇敢になり、団結と大多数を勝ち取ることに着眼し、理をもって有利に段階を追って輿論闘争を繰り広げ、幹部大衆が是非の境界をはっきり分け、あいまいな認識をはっきりさせることを支援しなければならない。悪意をもって党の指導を攻撃し、社会主義制度を攻撃し、党史国史を歪曲し、デマを流し、事を起こすあれらの言論に対しては、すべての新聞雑誌、講演論壇、会議会場、映画テレビ、ラジオ局、舞台劇場などいずれもそれらに空間を提供してはならず、すべてのデジタル新聞雑誌、移動テレビ、ケータイメディア、ケータイショートメール、マイクロメール、ブログ、Podcast、マイクロブログ、BBS などのニューメディアもいずれもそれに便宜を提供してはならない。こうした言論に対しては、ネット上で規制を強化しなければならないのみならず、着実に人への働きかけを行わなければならない。四つの基本原則に違反したものは、教育誘導しなければならず、責任制をつくらなければならず、所在場所と単位は確実に管理しなければならない。デマを流し、事を起こしたものに対しては、必ず法に基づいて調査処理しなければならず、「三岔口」のように暗闇の中で動き回るようなことをしてはならないし、こうした者にそこで勝手気ままにデマを流し、事を起こし、どさくさに紛れて利益を得、煽り立て、たきつけ、言いたい放題させてはならない。

（原文）

要敢抓敢管，敢于亮剑，着眼于团结和争取大多数，有理有利有节开展舆论斗争，帮助干部群众划清是非界限、澄清模糊认识。对那些恶意攻击党的领导、攻击社会主义制度、歪曲党史国史、造谣生事的言论，一切报刊杂志、讲台论坛、会议会场、电影电视、广播电台、舞台剧场等都不能为之提供空间，一切数字报刊、移动电视、手机媒体、手机短信、微信、博客、播客、微博客、论坛等新兴媒体都不能为之提供方便。对这些言论，不仅要在网络上加强控制，而且要落地做人的工作。对违反四项基本原则的，必须教育引导，要建立责任制，所在地方和单位要切实管起来；对造谣生事的，必须依法查处，不能像《三岔口》里那样摸着黑打来打去，也决不能让这些人在那里舒舒服服造谣生事、浑水摸鱼、煽风点火、信口雌黄。

・・・・・・・・・・

インターネットはすでに輿論闘争の主戦場になっている。ある同志が言うには、インターネットはわれわれが直面する「最大の変数」になっていて、うまく行わなければわれわれの「頭痛の種」になってしまう。西側反中勢力はずっとインターネットを利用して「中国を倒す」ことを企んできた。何年も前「インターネットをもつことになり、中国に対応する方法を得た」、「社会主義国家が西側の懐に飛び込むのに、インターネットから始まるであろう」と公言した西側の政治家がいた。米国の「ＰＲＩＳＭ」、「ｘ keyscore」などの監視計画から見ると、彼らのインターネット活動のエネルギーと規模は人の想像をはるかに超えたものである。インターネットというこの戦場で、われわれがもちこたえ、勝利できるか否かは直接我が国のイデオロギーの安全と政権の安全に関係する。

（原文）

互联网已经成为舆论斗争的主战场。有同志讲，互联网是我们面临的“最大变量”，搞不好会成为我们的“心头之患”。西方反华势力一直妄图利用互联网“扳倒中国”，多年前有西方政要就声称“有了互联网，对付中国就有了办法”，“社会主义国家投入西方怀抱，将从互联网开始”。从美国的“棱镜”、“X—关键得分”等监控计划看，他们的互联网活动能量和规模远远超出了世人想象。在互联网

这个战场上，我们能否顶得住、打得赢，直接关系我国意识形态安全和政权安全。

・・・・・・・・・・

情勢の発展の必要に基づけば、わたしはネット上での輿論工作を宣伝思想工作の重要な中でも重要として力を入れなければならないと見ている。宣伝思想工作は人への工作であり、人がどこにいるかによってそこが重点となるべきである。わが国のネット利用者は6億人近くであり、ケータイネット利用者は4.6億余人であり、そのうちウェイポーユーザーは3億余人に達している。たくさんの人、特に若い人は基本的に主流メディアを見ず、大部分の情報をネット上から得ている。この事実を直視し、力を強め投入し、速やかにこの輿論の戦場の主導権を掌握しなければならず、はじに追いやられてはならない。「本領パニック」問題をうまく解決し、真に現代メディアの新しい手段新しい方法を運用できるプロの専門家にならなければならない。深く掘り下げてネット上の世論闘争を繰り広げ、ネット上での攻撃浸透行為を厳密に防止し、力を組織し誤った思想的観点に対し批判反駁を行わなければならない。法に従ってネット社会管理を強化し、ネットの新しい技術新しい応用の管理を強化し、インターネットの管理ができコントロールできるを確保し、われわれのネット空間をすがすがしいものにしなければならない。この仕事をやるのは容易ではないが、難しくてもやらなければならない。天下に難き事なし、ただ心あるものを恐れる。他人が何を言おうが恐れるな。ネット上でマイナス面の言論が少なくなるのはわが国社会の発展、社会の安定、人民が落ち着いて暮らし仕事に励むことに対し、好いところだけで悪いところはない。わたしが往時生産隊に入っていた時の農民のことばを使えば、ケラが鳴くのを聞き作物を植えないほど恐れてはならない。

（原文）

根据形势发展需要，我看要把网上舆论工作作为宣传思想工作的重中之重来抓。宣传思想工作是做人的工作的，人在哪儿重点就应该在哪儿。我国网民有近6亿人，手机网民有4.6亿多人，其中微博用户达到3亿多人。很多人特别是年轻人基本不看主流媒体，大部分信息都从网上获取。必须正视这个事实，加大力量投入，尽快掌握这个舆论战场上的主动权，不能被边缘化了。要解决好“本领恐慌”问题，真正成为运用现代传媒新手段新方法的行家里手。要深入开展网上舆论斗争，严密防范和抑制网上攻击渗透行为，组织力量对错误思想观点进行批驳。要依法加强网络社会管理，加强网络新技术新应用的管理，确保互联网可管可控，使我们的网络空间清朗起来。做这项工作不容易，但再难也要做。天下无难事，只怕有心人。不要怕别人说什么。网上负面言论少一些，对我国社会发展、社会稳定、人民安居乐业只有好处没有坏处。用我当年插队时农民的话来说，不要听蝲蝲蛄叫就怕得不种庄稼了。

・・・・・・・・・・

われわれの同志は必ず陣地意識を強めなければならない。宣伝、思想の陣地はわれわれが占領しなければ、人さまが占領する。私が見るに、思想の陣地は大体三つのゾーンがある。一つ目はレッドゾーン、主に主流メディアとネット上の正面の勢力で構成されているもので、これはわれわれの主陣地であり、必ずしっかりと守り、決して失ってはならない。二つ目はブラックゾーンであり、主にネット上と社会の一部マイナス面の言論によって構成されているもので、それには各種敵対勢力が作り出した輿論を含んでおり、これは主流ではないがその影響を低く見積もってはならない。三つめはグレーゾーンであり、レッドとブラックの間にある。異なるゾーンに対しては、異なる策

略を取らなければならない。レッドゾーンに対しては、打ち固め発展させ、絶えずその社会的影響を拡大しなければならない。ブラックゾーンに対しては、勇敢に進入し、中核に潜り込み闘い、それが色を変えるよう徐々に推進しなければならない。グレーゾーンに対しては、大規模に活動を展開し、速やかにそれをレッドゾーンに転化させ、それがブラックゾーンに脱皮することを防止しなければならない。こうした活動は、しっかりと力を入れて行い、堅持していけば必ず成果を上げることができる。

（原文）

我们的同志一定要增强阵地意识。宣传思想阵地，我们不去占领，人家就会去占领。我看，思想舆论领域大致有 3 个地带。第一个是红色地带，主要是主流媒体和网上正面力量构成的，这是我们的主阵地，一定要守住，决不能丢了。第二个是黑色地带，主要是网上和社会上一些负面言论构成的，还包括各种敌对势力制造的舆论，这不是主流，但其影响不可低估。第三个是灰色地带，处于红色地带和黑色地带之间。对不同地带，要采取不同策略。对红色地带，要巩固和拓展，不断扩大其社会影响。对黑色地带，要勇于进入，钻进铁扇公主肚子里斗，逐步推动其改变颜色。对灰色地带，要大规模开展工作，加快使其转化为红色地带，防止其向黑色地带蜕变。这些工作，要抓紧做起来，坚持下去，必然会取得成效。

・・・・・・・・・・

ネット上での闘争は、一種の新しい輿論闘争の形態であり、戦略戦術を工夫しなければならない。人さまが運動戦、遊撃戦できているのに、われわれは正規戦、陣地戦だけで戦ってはならず、機動的柔軟にならなければならず、人さまの戦い方にわれわれは合わせ、真っ向から対峙し、機先を制し勝たなければならず、人さまの言いなりになって動いてはならず、戦術が単調であることで戦略という大局を誤ってはならない。これこそは「是は常に是といえども、時に用いず。非は常に非といえども、時に必ず行う」というものである。ネット上の闘争の特色と法則を深く掘り下げて分析し、ネット上での闘争の勢力を細心に組織しなければならない。ネットのオピニオンリーダーに対しては、教育誘導を強めなければならず、よい者は励まさなければならず、よくない者は拘束しなければならず、そのまま放任してはならない。

（原文）

网上斗争，是一种新的舆论斗争形态，必须讲究战略战术。人家打运动战、游击战，我们也不能只打正规战、阵地战，要机动灵活，人家怎么打我们就怎么打，针锋相对，出奇制胜，不能被人家牵着鼻子走，不能因为战术刻板而耽误战略大局。这就是：“是虽常是，有时而不用；非虽常非，有时而必行。”要深入分析网上斗争的特点和规律，精心组织网上斗争力量。对网络意见领袖，要加强教育引导，好的要鼓励，不好的要管束，不能放任自流。

・・・・・・・・・・

網掛け部分が 2014 年 5 月 28 日に中央文献出版社から出版された『习近平关于全面深化改革论述摘编』（中共中央文献研究室编辑）の「七、深化文化体制改革，加强社会主义核心价值体系建设」の中で初めて公表された内容である。

以上の習近平のインターネットに関係する発言を見ると、少なくとも政治的権利としての「言論、表現の自由」については「サイバー法」は厳格に用いられるであろう。しかし、中国と各国と

の経済交流の領域では、それが条文通り運用されるとすれば、摩擦が頻発することは疑いのないところである。

中国は 2016 年 12 月 27 日に「国家サイバー空間セキュリティ戦略」(《国家网络空间安全战略》)、また翌 2017 年 3 月 1 日には「サイバー空間国際協力戦略」(《网络空间国际合作战略》) を公表している。「輿論闘争の主戦場」としてのサイバー空間は中国においては、その「戦略」と「国際標準」とのせめぎ合いの「戦場」として、中国共産党によってそれが政治情報と経済情報とにかかわらず常に管理され続けるのであろう。その法的根拠が「中華人民共和国サイバーセキュリティー法」なのである。

最後に、本稿執筆にあたり、関係資料を高見澤学氏と仁田脇申一氏から提供を受けたので、ここに感謝申し上げる。

資料　中華人民共和国サイバーセキュリティー法

1.（日本語訳）中華人民共和国サイバーセキュリティー法
2.（中国語原文）中华人民共和国网络安全法

本法の日本語訳は徐淼、孫鑫鈺、席珺琳、毛雷、李一琳が担当、ネイティブチェックは田上雄大が行い、蔡昕悦が整理した。

なお、日本語訳の網かけの部分は第二次草案において、また下線“……”は成案となった際に加えられた内容である。

（日本語訳）

中華人民共和国サイバーセキュリティー法

（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で採択）

目　録

第一章　総　則
第二章　サイバーセキュリティーのサポートと促進
第三章　ネットワークの運用安全
　第一節　一般規定
　第二節　基幹情報インフラの運用安全
第四章　ネットワークの情報安全
第五章　モニタリング事前警報と応急処置
第六章　法的責任
第七章　附　　則

第一章　総　則

第一条　サイバーセキュリティーを保障し、サイバースペース主権及び国家の安全、社会の公共利益を守り、公民、法人及びその他の組織の合法的権益を保護し、経済社会情報化の健全な発展を促進するため、本法を制定する。

第二条　中華人民共和国域内でネットワークを建設、運営、維持、使用すること、及びサイバーセキュリティーの監督管理には、本法を適用する。

第三条　国家はサイバーセキュリティーと情報化の発展を同様に重んじることを堅持し、積極的に利用し、科学的に発展させ、法に基づき管理し、安全を確保するという方針を遵守し、ネットワークインフラの建設と相互接続を推進し、ネットワーク技術のイノベーションと応用を鼓舞し、サイバーセキュリティーの人材を養成することをサポートし、健全なサイバーセキュリティー保障体系を確立、サイバーセキュリティー保護能力を向上させる。

第四条　国家は、サイバーセキュリティー戦略を制定するとともに、絶えず完備させ、サイバーセキュリティーを保障する基本要求と主要目標を明確にし、重点領域のサイバーセキュリティー政策、活動任務と措置を提起する。

第五条　国家は、措置を講じて中華人民共和国域内外からのサイバーセキュリティーリスクと脅威をモニタリング・防御・処置し、基幹情報インフラが攻撃、侵入、妨害、及び破壊を受けないようするため保護し、法に基づきネットワーク違法犯罪活動に懲罰を与え、サイバースペース安全と秩序を守る。

第六条　国家は、誠実に信用を守り、健全で文明的なネットワーク行為を唱導し、社会主義の核心的価値観の伝播を推し進め、措置を講じて全社会のサイバーセキュリティー意識と水準を向上させ、全社会が共同でサイバーセキュリティーに参与し、促進するという良好な環境を作り出す。(1)

第七条　国家は、積極的に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に打撃を与えることなどにおける国際交流と協力を展開し、平和、安全、開放、協力のサイバースペースの構築を推し進め、多角的、民主的、透明なネットワークのガバナンス体系を確立する。(2)

第八条　国家ネットワーク情報部門は、サイバーセキュリティー活動と関連する監督管理活動を統括調整する責任を負う。国務院電信主管部門、公安部門及びその他の関係機関は本法と関係法律、行政法規の規定に基づき、それぞれの職責範囲内でサイバーセキュリティー保護と監督管理活動の責任を負う。(3)

県級以上の地方人民政府における関係部門のサイバーセキュリティー保護と監督管理の職責は国家の関係規定に照らして確定される。

第九条　ネットワーク運営者は、経営及びサービス活動を展開するには、法律、行政法規を遵守し、社会公徳を尊重し、商業道徳、信義誠実を遵守し、サイバーセキュリティー保護義務を履行し、政府と社会の監督を受け入れ、社会責任を負わなければならない。

第十条　ネットワークの建設、運営また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、業界標準の強制的要求に基づいて、技術措置とその他の必要な措置を講じ、サイバーセキュリティー、安定的運用を保障し、サイバーセキュリティー事件に効果的に対応し、違法犯罪活動を防止し、ネットワークデータの保全性、秘密性と利用可能性を維持すべきである。(4)

第十一条　ネットワーク関連の業種組織は規程に基づき、業種の自律を強化し、サイバーセキュリティー行為規範を制定し、会員を指導し、サイバーセキュリティー保護を強化し、サイバーセキュリティー保護水準を向上させ、業種が健全に発展するように促進する。(5)

第十二条　国家は、公民、法人とその他の組織が法に基づき、ネットワークを使用する権利を保護し、ネットワークへの接続を普及することを促進し、ネットワークサービス水準を引き上げて、社会に安全、便利なネットワークサービスを提供するために、ネットワーク情報が法に基づき秩序立って自由に流通されることを保障する。(6)

いかなる個人や組織も、ネットワークを使用するには、憲法、法律を遵守し、公共秩序を遵守し、社会公徳を尊重すべきであり、サイバーセキュリティー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、栄誉および利益に危害を加え、国家政権の転覆、社会主義制度の打倒の煽動、国家の分裂、国家の統一の破壊の煽動、テロリズムと過激主義の宣揚、民族憎悪と民族差別の宣揚、猥褻色情情報の伝播、嘘の情報を編成、伝播することによって経済秩序および社会秩序を混乱させ、他人の名誉、プライバシー、知的財産権とその他の合法的な権益を侵害するなどの活動に従事してはならない。

第十三条　国家は、未成年者が健全に成長するのに有益となるネットワーク製品とサービスの研究開発をサポートし、法に基づき、ネットワークを利用して未成年者の心身の健康に危害を与える活動に懲罰を与え、未成年者に安全、健全なネットワーク環境を提供する。

第十四条　いかなる個人や組織も、サイバーセキュリティーに危害を加える行為に対してネットワーク情報、電信、公安などの部門に摘発する権利がある。摘発を受けた部門は、ただちに法に基づき処理すべきである。当該部門の職責に属さないものは、ただちに処理の権限をもつ部門に移管すべきである。(7)

関連部門は、摘発者の関連情報に対してその秘密を守り、摘発者の合法的権益を保護すべきである。

第二章　サイバーセキュリティーサポートと促進

第十五条　国家は、サイバーセキュリティー標準体系を確立し、整備する。国務院標準化行政主管部門と国務院のその他の関係部門は、それぞれの職責に基づいて、サイバーセキュリティー管理及びネットワーク製品、サービスと運用安全に関係する国家標準、業種標準を組織制定するとともに、しかるべきときに改訂する。(8)

国家は、企業、研究機関、高等教育機関、ネットワーク関連の業種組織がサイバーセキュリティーの国家標準、業種標準の制定に参与することをサポートする。

第十六条　国務院は、省、自治区、直轄市人民政府と全体を統括調整し、投資を拡大し、重点サイバーセキュリティー技術産業とプロジェクトを扶助し、サイバーセキュリティー技術の研究開発と応用をサポートし、安全で信頼されるネットワーク製品とサービスを普及させ、ネットワーク技術知的財産権を保護し、企業、研究機関と高等教育機関などが国家サイバーセキュリティー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すべきである。(9)

第十七条　国家は、サイバーセキュリティーの社会化サービスシステムの建設を推進し、関係企業、機関がサイバーセキュリティー認証、測定とリスク評価など安全サービスを行展開することを鼓舞する。

第十八条　国家は、ネットワークデータの安全保護と利用技術を開発するのを鼓舞し、公共のデータ資源の開放を促進し、技術のイノベーションと経済社会の発展を推し進める。

国家は、サイバーセキュリティーの管理方式のイノベーションをサポートし、ネットワーク新技術を運用し、サイバーセキュリティー保護の水準を引き上げる。

第十九条　各級人民政府及びその関係部門は、経常的なサイバーセキュリティー宣伝教育を組織し、展開するとともに、関係単位がうまくサイバーセキュリティー宣伝教育活動を行うことを指導、督促すべきである。(10)

マス・メディアは、明確な対象を持って、社会に向けて、サイバーセキュリティー宣伝教育を行うべきである。

第二十条　国家は、企業が高等教育機関、専門学校などの教育訓練機関とサイバーセキュリティーに関する教育と訓練を繰り広げ、さまざまな方式を講じ、サイバーセキュリティーの人材を養成し、サイバーセキュリティーの人材交流を促進することをサポートする。(11)

第三章　ネットワーク運用安全

第一節　一般規定

第二十一条　国家は、サイバーセキュリティー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ー等級保護制度の要求に合わせて、下記の安全保護の義務を履行し、ネットワークが妨害、破壊または権限を得ずして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洩、または窃取、改竄を防止すべきである。(12)

（一）　内部の安全管理制度と操作規定を制定し、サイバーセキュリティーの責任者を確定し、サイバーセキュリティー保護の責任を明確にする。

（二）　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サイバーセキュリティーに

危害を及ぼす行為を防止できる技術的措置を講じる。

（三） ネットワーク運用状態とサイバーセキュリティー事件をモニタリングし、記録する技術的措置を講じるとともに、規定に従って、関係ブログを六ヶ月を下回らないように保存する。

（四） データを分類し、重要なデータをバックアップし、暗号化するなどの措置を講じる。

（五） 法律、行政法規に規定されているその他の義務。

第二十二条 ネットワーク製品、サービスは、関係する国家標準の強制的要求と合致させるべきである。ネットワーク製品、サービスの提供者は、悪意のあるプログラムを設置してはならない。そのネットワーク製品、サービスに安全上の欠陥、不備などのリスクがあることを発見したら、すぐに補完措置を講じて、規定に従って適時にユーザーに告示するとともに、関係主管部門に報告すべきである。(13)

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、引き続き安全維持の提供をすべきであり、規定または当事者の取り決めの期限内に、安全維持の提供を終了してはならない。

ネットワーク製品、サービスにユーザー情報の収集機能がある場合、その提供者は、ユーザーに明示する共に、同意を得るべきである。ユーザーの個人情報にかかわる場合、さらに、本法と関連の法律、行政法規の個人情報に関する規定も遵守すべきである。

第二十三条 ネットワークの基幹設備とサイバーセキュリティーの専用製品は、関係する国家の標準の強制的要求に合わせるべきであり、資格を備える機関によって安全認証に合格した、または安全検査測定の要求と合致した後、はじめて販売または提供できる。国家ネットワーク情報部門は、国務院の関係部門とともにネットワークの基幹設備とサイバーセキュリティーの専用製品のカタログを作り、公布するとともに、安全認証と安全検査測定の結果の相互認証を推進して、認証、検査測定の重複を回避させる。(14)

第二十四条 ネットワーク運営者は、ユーザーのためにネットワーク接続、ドメイン名登録サービスを行い、固定電話、携帯電話などのプロバイダ加入手続きを行い、またはユーザーのために情報の公表、インスタントメッセージなどのサービスを提供するうえで、ユーザーと取り決めを結ぶかまたは提供するサービスを確認するとき、ユーザーに真実の身分情報を提供することを要求すべきである。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、関連サービスをそれに提供してはならない。(15)

国家は、ネットワークの信頼できる身分戦略を実施し、安全、便利な電子身分情報認証技術の研究と開発をサポートし、異なる電子身分認証間の相互認証を推し進める。

第二十五条 ネットワーク運営者は、サイバーセキュリティー事件応急マニュアルを制定し、適時にシステムのバグ、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安全リスクに対処すべきである。サイバーセキュリティーに危害を及ぼす事件が発生したとき、ただちに応急マニュアルを起動し、それに応じた補完措置を講じると同時に、規定に従って関係主管部門に報告すべきである。(16)

第二十六条 サイバーセキュリティー認証、測定、リスク評価などの活動を展開するうえで、社会に向けて、システムのバグ、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ー情報を公表する際、国家の関係規定を遵守すべきである。

第二十七条 いかなる個人や組織も、不法に他人のネットワークに侵入すること、他人のネット

ワークの正常な機能を妨げること、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ーに危害を及ぼす活動に従事してはならない。ネットワークに侵入すること、ネットワークの正常な機能を妨げること、ネットワークデータを摂取するなどのサイバーセキュリティー活動に危害を及ぼすプログラム、デバイスを提供してはならない。サイバーセキュリティーに危害を及ぼす活動に他人が従事していることが明らかになった場合、それに技術的サポート、広告普及、支払決算などの援助を行なってはならない。(17)

第二十八条　ネットワーク運営者は、公安機関、国家安全機関の法に基づき国家安全を守ることと犯罪事件を捜査する活動のために、技術的サポートと協力を提供すべきである。

第二十九条　国家は、ネットワーク運営者の間でサイバーセキュリティー情報収集、分析、通報及び応急措置などの面で協力が展開することをサポートし、ネットワーク運営者の安全保障能力を向上させる。(18)

関連業種組織は、当該業種のサイバーセキュリティー保護規範と連携メカニズムを構築し、サイバーセキュリティーリスクに対する分析と評価を強化し、定期的に会員にリスク警告を行い、会員のサイバーセキュリティーリスク対応をサポート、協力する。

第三十条　ネットワーク情報部門と関係部門は、サイバーセキュリティー保護の職責を履行するときに得た情報をサイバーセキュリティーを守るためにのみ、必要に応じて使用でき、その他の用途に使ってはならない。

第二節　基幹情報インフラの運用安全

第三十一条　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な業種と領域及びその他の一旦破壊され、機能を失ったか、またはデータの漏洩によって、国家の安全、国民の経済と人民生活、公共の利益に重大な脅威を与える可能性のある基幹情報インフラに対し、サイバーセキュリティー等級保護制度を基礎にして、重点的保護を実行する。基幹情報インフラの安全保護の弁法は、国務院によって制定される。(19)

国家は、基幹情報インフラ以外のネットワーク運営事業者が自発的に基幹情報インフラ保護体系に参与するよう鼓舞する。

第三十二条　国務院の規定する職責分業に従って、基幹情報インフラの安全保護業務の責任を負う部門は、それぞれ当該業種、当該領域における基幹情報インフラの安全の計画を編制するとともに、組織実施して、基幹情報インフラの運用安全を保護する業務を指導し、監督する。(20)

第三十三条　基幹情報インフラを建設するには、それが業務の安定、持続的運用をサポートする性能を持つことを確保するとともに、安全技術の措置が同時に計画、同時に建設、同時に使用されることを保証すべきである。(21)

第三十四条　本法第二十一条の規定以外、基幹情報インフラの運営者は下記の安全保護の義務も履行すべきである。(22)

（一）　専門的な安全管理機関と安全管理の責任者を置くとともに、当該責任者と重要なポストの人員に対して、安全背景の審査を行う。

（二）　定期的に従業員に対してサイバーセキュリティーの教育、技術の訓練と技能の考課を行う。

（三）　重要なシステムとデータベースに対して被災予備のバックアップを行う。

（四）　サイバーセキュリティー事件の応急マニュアルを制定し、あわせて定期的に予行演習を行

う。

（五） 法律、行政法規によって規定されたその他の義務。

第三十五条 基幹情報インフラの運営者は、ネットワークの製品購入またはサービスをするにあたって、国家の安全に影響を与える可能性がある場合、国家のネットワーク情報部門は、国務院の関連部門と組織した安全審査を通すべきである。(23)

第三十六条 基幹情報インフラの運営者は、ネットワークの製品購入とサービスをするには、規定に従って提供者と安全秘密保護取決めに調印し、安全と秘密保護の義務と責任を明確すべきである。(24)

第三十七条 基幹情報インフラの運営者は、中華人民共和国域内で運営中に収集、生まれた公民の個人情報と重要なデータを域内に保存すべきである。業務の需要のため、確かに域外に提供する必要がある場合は、国家のネットワーク情報部門が国務院の関連部門とともに制定した方法によって安全評価を行うべきである。法律、行政法規に別に規定がある場合は、その規定に従う。(25)

第三十八条 基幹情報インフラの運営者は、自主的またはサイバーセキュリティーのサービス機関に委ねて、そのネットワークの安全性と存在する可能性のあるリスクに対して、毎年少なくとも一回の測定評価を行うとともに、測定評価の状況及び改善措置については、関連基幹情報インフラの安全保護の業務に責任を負う部門に報告すべきである。(26)

第三十九条 国家のネットワーク情報部門は、関連部門を統括調整すべきであり、基幹情報インフラの安全保護に対して、下記の措置を講じるべきである。(27)

（一） 基幹情報のインフラの安全リスクに対して抜き取り検査測定を行って、改善措置を提起し、必要な時にはサイバーセキュリティーサービス機関に委ね、ネットワークに存在している安全リスクに対して測定評価を行うことができる。

（二） 定期的に基幹情報インフラの運営者を組織して、サイバーセキュリティー応急の予行演習を行い、サイバーセキュリティー事件に対応できる水準と協力能力を向上させる。

（三） 関連部門、基幹情報インフラの運営者及び関連研究機関、サイバーセキュリティーサービス機関などの間のサイバーセキュリティー情報の共有を促進する。

（四） サイバーセキュリティー事件の応急措置とネットワーク機能回復などに対して、技術的サポートと協力を提供する。

第四章 ネットワークの情報安全

第四十条 ネットワーク運営者は、収集したユーザーの情報に対して厳格に秘密を保護すべきであり、あわせてユーザー情報の保護制度を確立、健全にすべきである。(28)

第四十一条 ネットワーク運営者が個人情報を収集または使用するには、合法、正当、必要の原則を遵守し、情報を収集、使用する目的、方法及び範囲を明示するとともに、被収集者の同意を経るべきである。(29)

ネットワーク運営者は、その提供するサービスに関係がない個人情報を収集してはならず、個人情報を使用または収集するには法律、行政法規の規定と双方の契約に違反してはならず、あわせて法律、行政法規の規定またはユーザーとの契約に基づいて、その保存した個人情報を処理すべきである。

第四十二条 ネットワーク運営者は、収集した個人情報を漏洩、改竄、棄損してはならず、被収

集者の同意を経ずに、他人に個人情報を提供してはならない。しかし、処理を経て識別できない特定の個人情報かつ復元できない場合を除く。

ネットワーク運営者は、技術的措置やその他の必要な措置を講じて、公民の個人情報の安全を確保し、収集した個人情報が漏洩、棄損、紛失することを防止すべきである。情報の漏洩、棄損、紛失が発生または発生する可能性が生じた場合、ただちに救済措置を講じ、影響を受ける可能性のあるユーザーに告知するとともに、規定に従って関係主管部門に報告すべきである。

第四十三条　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契約に違反し、その個人情報を収集または使用したのを発見したら、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がある。ネットワーク運営者の収集または保存した個人情報に誤りがあるのを発見したら、ネットワーク運営者に訂正を要求する権利がある。ネットワーク運営者は措置を講じて誤りを削除または訂正すべきである。(30)

第四十四条　いかなる個人や組織も、窃盗または他の違法な方法を用いて、公民の個人情報を得てはならず、他人に公民の個人情報を販売または提供してはならない。(31)

第四十五条　法律によりネットワークワーク安全監督管理の職責を負う部門及び職員は、職責を履行する際に知り得た公民の個人情報、プライバシー、ビジネス秘密に対して厳格に秘密を保護しなければならず、個人情報を漏洩、販売または違法に他人に提供してはならない。(32)

第四十六条　いかなる個人や組織も、ネットワークを使用する行為に責任を負うべきであり、詐欺の実行、犯罪方法の伝授、違法製品、規制製品の製作または販売などの違法、犯罪活動に用いるウェブサイト、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、詐欺の実行、違法製品または規制製品の製作または販売とその他の違法、犯罪活動に関係する情報を公表してはならない。

第四十七条　ネットワーク運営者は、そのユーザーが発表する情報の管理を強化するべきであり、法律、行政法規により公表または伝送が禁止された情報を発見したら、当該情報の伝送をすぐに停止し、削除などの措置を講じ、情報の拡散を防止し、関係記録を保存するとともに関係主管部門に報告すべきである。(33)

第四十八条　いかなる個人や組織も、配信する電子情報、提供する応用ソフトに悪意あるプログラムを設定してはならず、法律、行政法規により公表、伝送の禁止されている情報を含んではならない。

電子情報の配信サービス提供者と応用ソフトのダウンロードサービス提供者は、安全管理の義務を履行すべきであり、そのユーザーに前款の規定に違反する行為があることを知ったら、サービスの提供を停止すべきであり、削除など措置を講じ、関係記録を保存するとともに関係主管部門に報告すべきである。

第四十九条　ネットワーク運営者は、ネットワーク情報安全の苦情訴え、摘発プラットフォームをつくり、苦情訴え、摘発方式などの情報を公表し、適時に関係ネットワークワーク情報安全の苦情訴えと摘発を処理すべきである。(34)

ネットワーク運営者は、ネットワーク情報部門と関係部門が法により監督検査を実行することに対しそれに協力すべきである。

第五十条　国家ネットワーク情報部門と関係部門は、法に基づきネットワークの情報安全監督の管理責任を履行するにあたり、法律、行政法規により発表、伝送の禁止されている情報を発見した

ら、ネットワーク運営者にその情報の伝送を停止し、削除など措置を講じ、関係記録を保存するよう要求すべきである。中華人民共和国域外からきた上記情報に対して、関係機関は、技術的措置やその他の必要な措置を講じて情報の伝播を遮断するよう通知すべきである。(35)

第五章　モニタリング事前警報と応急処置

第五十一条　国家は、サイバーセキュリティーのモニタリング事前警報と情報通報制度を構築する。国家ネットワーク情報部門は関係部門を統一的に統括調整してサイバーセキュリティー情報の収集、分析及び通報活動を強化し、規定に従ってサイバーセキュリティーのモニタリング事前警報情報を統一して発表すべきである。(36)

第五十二条　基幹情報インフラの安全保護業務の責任を負う部門は、当該業種、当該領域におけるサイバーセキュリティーのモニタリング事前警報と情報通報制度を構築、完備させるとともに、規定に従ってサイバーセキュリティーのモニタリング事前警報情報をとどけるべきである。(37)

第五十三条　国家ネットワーク情報部門は、関係部門を調整してサイバーセキュリティーのリスク評価と応急活動メカニズムを構築、完備させ、サイバーセキュリティー事件の応急マニュアルを制定するとともに、定期的に予行演習を組織する。(38)

基幹情報インフラの安全保護業務の責任を負う部門は、当該業種、当該領域におけるサイバーセキュリティー事件の応急マニュアルを制定するとともに、定期的に予行演習を組織すべきである。

サイバーセキュリティー事件の応急マニュアルは、事件が発生したあとの危害程度、影響範囲などの要素に基づいて、サイバーセキュリティー事件に対して等級をつけるとともに、対応する応急措置を規定すべきである。

第五十四条　サイバーセキュリティー事件発生の可能性が増大したら、省級以上の人民政府の関係部門は、規定する権限と手順に従い、あわせてサイバーセキュリティーリスクの特徴ともたらさせられるであろう危害に基づいて、下記の措置を講じるべきである。(39)

（一）　関係部門、機関と人員に適時に関係情報を収集、報告し、サイバーセキュリティー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）　関係部門、機関と専門人員を組織し、サイバーセキュリティーリスク情報に対して分析評価を行い、事件が発生する可能性、影響範囲及び危害程度を予測する。

（三）　社会にサイバーセキュリティーリスクの事前警報を公表し、危害を回避、軽減する措置を公表する。

第五十五条　サイバーセキュリティー事件が発生したら、ただちにサイバーセキュリティー事件の応急マニュアルを起動し、サイバーセキュリティー事件に対して調査と評価を行い、ネットワーク運営者に技術的な措置及びその他の必要な措置を講じ、安全の隠れた災いを取り除き、危害の拡大を防ぐとともに、適時に公衆に関わる警告情報を社会に公表するよう要求すべきである。(40)

第五十六条　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ー監督管理の職責を履行するなかで、ネットワークに比較的に大きい安全リスクが存在していたら、またはサイバーセキュリティー事件が起きたのを発見したら、規定する権限と手順に従い、当該ネットワークの運営者の法定代表者または主要な責任者に対して、事情聴取をすることができる。ネットワーク運営者は、要求に基づいて、措置を講じ、整頓改革を行い、隠れた災いを削除すべきである。

第五十七条　サイバーセキュリティー事件により、突発事件または生産安全事故が起きたら、

『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』などの関係法律、行政法規の規定に従って処置すべきである。(41)

第五十八条　国家安全と社会公共秩序を守り、重大な突発社会安全事件を処置する必要のため、国務院の決定または承認を経て、特定区域においてネットワーク通信に対して制限などの臨時の措置を講じることができる。(42)

第六章　法的責任

第五十九条　ネットワーク運営者が、本法第二十一条、第二十五条に規定されているサイバーセキュリティー保護義務を履行しない場合、関係主管部門によって、是正を命じられ、警告が与えられる。是正を拒否またはネットワークの安全に危害を及ぼすといった結果を惹起した場合、一万元以上十万元以下の罰金に処し、直接に責任を負う主管人員に対して、五千元以上五万元以下の罰金に処する。(43)

基幹情報インフラの運営者が、本法第三十三条、第三十四条、第三十六条及び第三十八条に規定されているサイバーセキュリティー保護義務を履行しない場合、関係主管部門によって、是正を命じられ、警告が与えられる。是正を拒否またはサイバーセキュリティーに危害を及ぼす結果を惹起した場合、十万元以上百万元以下の罰金に処し、直接責任を負う主管人員に対しては、一万元以上十万元以下の罰金に処する。

第六十条　本法第二十二条第一款及び第二款並びに第四十八条第一款の規定に違反し、以下の行為のいずれかに該当する場合、関係主管部門によって、是正を命じられ、警告が与えられる。是正を拒否またはネットワークの安全に危害を及ぼす結果を惹起した場合、五万元以上五十万元以下の罰金に処し、直接責任を負う主管人員に対して、一万元以上十万元以下の罰金に処する。(44)

（一）　ウイルスを設置した場合。

（二）　その製品、サービスに存在するセキュリティ上の欠陥、セキュリティホール等のリスクに対して、ただちに救済措置を講じない、または規定に沿って適時にユーザーに告知しないとともに関係主管部門に報告をしない場合。

（三）　その製品、サービスに提供される安全保護を勝手に終了した場合。

第六十一条　ネットワーク運営者が本法第二十四条第一款の規定に違反し、ユーザーに正しい身分情報の提供を要求しない、または正しい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、関係主管部門によって是正を命じられる。是正を拒否または情状が重大である場合、五万元以上五十万元以下の罰金に処するとともに、関係主管部門によって、関連業務停止、業務停止整理、サイト閉鎖、関連業務許可証取上げまたは営業免許取消しが命じられ、直接責任を負う主管人員及びその他の直接責任者に対して、一万元以上十万元以下の罰金に処する。(45)

第六十二条　本法第二十六条の規定に違反し、サイバーセキュリティー認証、検査、リスク評価等の活動の展開、または社会にシステムホール、コンピュータウイルス、サイバー攻撃、ハッキング等のサイバーセキュリティー情報を公表した場合、関係主管部門によって、是正を命じられ、警告が与えられる。是正を拒否または情状が重大である場合、一万元以上十万元以下の罰金に処するとともに、関係主管部門によって、関連業務停止、業務停止整理、サイト閉鎖、関連業務許可証取上げまたは営業免許取消しが命じられ、直接責任を負う主管人員及びその他の直接責任者に対して、五千元以上五万元以下の罰金に処する。

第六十三条　本法第二十七条の規定に違反し、ネットワークの安全に危害を及ぼす活動への従事、または専らネットワークの安全に危害を及ぼす活動に従事するのに用いられるプログラム、デバイスを提供したり、若しくは他人がネットワークの安全に危害を及ぼす活動に従事するために、技術サポート、広告普及、決算支払等の援助を提供したもので、まだ犯罪を構成しない場合、公安機関によって違法所得を没収され、五日以内の拘留に処し、あわせて五万元以上五十万元以下の罰金に処する。情状が重大である場合、五日以上十五日以内の拘留に処し、あわせて十万元以上百万元以下の罰金に処する。

事業者が前款にある行為を行った場合、公安機関によって違法所得を没収され、十万元以上百万元以下の罰金に処し、あわせて直接責任を負う主管人員及びその他の直接責任者に対して、前款の規定に沿って処罰する。

本法第二十七条の規定に違反し、治安維持処罰を受けた人員は、五年間、サイバーセキュリティー維持及びネットワーク運営基幹職域の業務に従事してはならない。刑事処罰を受けた人員は、終身サイバーセキュリティー維持及びネットワーク運営基幹職の業務に従事してはならない。

第六十四条　ネットワーク運営者、ネットワーク製品またはサービス提供者が本法第二十二条第三款、第四十一条から第四十三条の規定に違反し、個人情報が法律によって保護される権利を侵害した場合、関係主管部門によって是正を命じられ、情状に応じて警告、違法所得没収、違法所得の倍以上十倍以下の罰金に処する事を単科または併科し、違法所得がない場合、百万元以下の罰金を処し、直接責任を負う主管人員及びその他の直接責任者に対して、一万元以上十万元以下の罰金に処することができる。情状が重大である場合、あわせて関連業務停止、業務停止整理、サイト閉鎖、関連業務許可証取上げまたは営業免許取消しが命じられる。(46)

本法第四十四条の規定に違反し、個人情報の窃取またはその他の方法による違法取得、違法販売または違法に他人へ提供をし、まだ犯罪を構成しない場合、公安部門によって違法所得が没収されるとともに、違法所得の倍以上十倍以下の罰金に処し、違法所得がない場合、百万元以下の罰金に処する。

第六十五条　基幹情報インフラの運営者が本法第三十五条の規定に違反し、安全審査を経ていないまたは安全審査に通らず且つネットワーク製品の使用またはサービスを行った場合、関係主管部門によって使用停止を命じられ、購入金額の倍以上十倍以下の罰金に処する。直接責任を負う主管人員及びその他の直接責任者に対しては、一万元以上十万元以下の罰金に処する。(47)

第六十六条　基幹情報インフラの運営者が本法第三十七条の規定に違反し、域外でのネットワークデータ保存、または域外へのネットワークデータ提供をした場合、関係主管部門によって、是正を命じられ、警告が与えられ、違法所得が没収され、五万元以上五十万元以下の罰金に処するとともに、関連業務停止、業務停止整理、サイト閉鎖、関連業務許可証取上げまたは営業免許取消しが命じられる。直接責任を負う主管人員及びその他の直接責任者に対しては、一万元以上十万元以下の罰金に処する。(48)

第六十七条　本法第四十六条の規定に違反し、違法犯罪活動の実行において用いられるサイト、通信グループの設立、または違法犯罪活動の実行に関係する情報を公表するためのネットワーク利用で、まだ犯罪を構成しない場合、公安機関によって五日以内の拘留に処し、あわせて一万元以上十万元以下の罰金に処する。情状が重大である場合、五日以上十五日以内の拘留に処し、あわせて

五万元以上五十万元以下の罰金に処する。違法犯罪活動に用いたサイト、通信グループを閉鎖する。

単位が前款にある行為を行った場合、公安機関によって十万元以上五十万元以下の罰金に処し、あわせて直接責任を負う主管人員及びその他の直接責任者に対して、前款の規定に従って処罰する。

第六十八条　ネットワーク運営者が本法第四十七条の規定に違反し、法律、行政法規が公表または伝送を禁止した情報に対して伝送停止、削除等の措置を未だ講じず、関係記録を保存している場合、関係主管部門によって是正を命じられ、警告が与えられ、違法所得が没収される。是正を拒否または情状が重大である場合、十万元以上五十万元以下の罰金に処するとともに、関連業務停止、業務停止整理、サイト閉鎖、関連業務許可証取上げまたは営業免許取消しが命じられ、直接責任を負う主管人員及びその他の直接責任者に対して、二万元以上二十万元以下の罰金に処する。(49)

電子情報送信サービス提供者、応用ソフトウェアのダウンロードサービス提供者が、本法第四十八条第二款の規定の安全管理義務を履行しない場合、前款の規定に従って処罰する。

第六十九条　ネットワーク運営者が本法の規定に違反し、以下の行為のいずれか一つがあった場合、関係主管部門によって是正を命じられる。是正を拒否または情状が重大である場合、五万元以上十万元以下の罰金に処し、直接責任を負う主管人員及びその他の直接責任者に対しては、一万元以上十万元以下の罰金に処する。(50)

（一）関係部門の要求によらず法律、行政法規が公表または伝送を禁止している情報に対して、伝送停止、削除等の措置を講じなかった場合。

（二）関係部門が法律に従って実施する監督、検査を拒否、妨害した場合。

（三）公安機関、国家安全機関に技術サポート及び協力の提供を拒否した場合。

第七十条　本法第十二条第二款及びその他の法律、行政法規が公表または伝送を禁止した情報を公表、伝送した場合、関係法律、行政法規の規定により処罰する。(51)

第七十一条　本法の規定する違法行為があった場合、関係法律、行政法規の規定に従って、信用ファイルに記入し、あわせて公示する。

第七十二条　国家政務機関のネットワーク運営者が本法に規定されるサイバーセキュリティー保護義務を履行しない場合、その上級機関または関係機関によって是正を命じられる。直接責任を負う主管人員及びその他直接責任者に対しては、法に従って処分を行う。(52)

第七十三条　ネットワーク情報部門及び関係部門が本法三十条の規定に違反し、且つサイバーセキュリティー保護の職責にある状態で取得した情報をその他の用途に用いた場合、直接責任を負う主管人員及びその他の直接責任者に対して、法に従って処分を行う。

ネットワーク情報部門及び関係部門の従業員が、職責怠慢、職権濫用、不正行為をし、まだ犯罪を構成しない場合、法に従って処分を行う。

第七十四条　本法規定に違反し、他人に損害を与えた場合、法に従って民事責任を負う。(53)

本法規定に違反したもので、治安管理に違反する行為を構成した場合、法に従って治安管理処罰を与える。犯罪を構成した場合、法に従って刑事責任を追究する。

第七十五条　域外の機関、組織、個人が攻撃、侵入、妨害、破壊等の危害を中華人民共和国の基幹情報インフラに与える活動をし、重大な結果を惹起する場合、法に従って法的責任を追究する。国務院公安部門及び関係部門は、あわせて当該機関、組織、個人に対して、財産凍結またはその他の必要な制裁措置を講じる決定を行う。

第七章　附　則

第七十六条　本法における下記の用語の意味：[54]

（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及び関連の設備によって構成され、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。

（二）　サイバーセキュリティーとは、必要な措置を講じることを通じて、ネットワークに対しての攻撃、侵入、妨害、破壊や不法使用及び不測のな事故を防止し、ネットワークを安定・信頼ある運用状態にさせるとともに、ネットワークデータの整合性、機密性、利用可能性の能力を保障することを指す。

（三）　ネットワーク運営者とは、ネットワークの所有者、管理者及びネットワークサービス提供者を指す。

（四）　ネットワークデータとは、ネットワークを通じ収集、保存、伝送、処理及び生産する各種の電子データを指す。

（五）　個人情報とは、電子またはその他の方式により記録された単独またはその他の情報と合わせて、自然人の個人の身分情報が識別できる各種の情報を指す。但し、自然人の氏名、生年月日、身分証明書の番号、個人生体識別情報、住所、電話番号などに限られない。

第七十七条　国家秘密に関わる情報を保存、処理するネットワークの運用安全保護は、本法を遵守する以外、秘密保護の法律、行政法規の規定も遵守すべきである。[55]

第七十八条　軍事ネットワークの安全保護は、中央軍事委員会により別に制定される。[56]

第七十九条　本法は2017年6月1日から施行する。[57]

（1）　草案第四条
（2）　草案第五条
（3）　草案第六条
（4）　草案第七条
（5）　草案第八条
（6）　草案第九条
（7）　草案第十条
（8）　草案第十三条
（9）　草案第十四条
（10）　草案第十五条
（11）　草案第十六条
（12）　草案第十七条
（13）　草案第十八条
（14）　草案第十九条
（15）　草案第二十条
（16）　草案第二十一条
（17）　草案第二十二条

(18) 草案第二十四条
(19) 草案第二十五条
(20) 草案第二十六条
(21) 草案第二十七条
(22) 草案第二十八条
(23) 草案第三十条
(24) 草案第二十九条
(25) 草案第三十一条
(26) 草案第三十二条
(27) 草案第三十三条
(28) 草案第三十四条
(29) 草案第三十五条
(30) 草案第三十七条
(31) 草案第三十八条
(32) 草案第三十九条
(33) 草案第四十条
(34) 草案第四十二条
(35) 草案第四十三条
(36) 草案第四十四条
(37) 草案第四十五条
(38) 草案第四十六条
(39) 草案第四十七条
(40) 草案第四十八条
(41) 草案第四十九条
(42) 草案第五十条
(43) 草案第五十一条
(44) 草案第五十二条
(45) 草案第五十三条
(46) 草案第五十四条
(47) 草案第五十五条
(48) 草案第五十六条
(49) 草案第五十七条
(50) 草案第五十九条
(51) 草案第五十八条
(52) 草案第六十一条
(53) 草案第六十三、六十四条
(54) 草案第六十五条
(55) 草案第六十六条

(56) 草案第六十七条

(57) 草案第六十八条

（中国語原文）

中华人民共和国网络安全法

（2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通过）

目　录

第一章　总　则
第二章　网络安全支持与促进
第三章　网络运行安全
　第一节　一般规定
　第二节　关键信息基础设施的运行安全
第四章　网络信息安全
第五章　监测预警与应急处置
第六章　法律责任
第七章　附　则

第一章　总　则

第一条　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。

第二条　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。

第三条　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。

第四条　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。

第五条　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。

第六条　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。

第七条　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。

第八条　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。

第九条　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。

第十条　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。

第十一条　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。

第十二条　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。

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。

第十三条　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。

第十四条　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。

第二章　网络安全支持与促进

第十五条　国家建立和完善（整備）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。

第十六条　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。

第十七条　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。

第十八条　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。

第十九条　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。

第二十条　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。

第三章　网络运行安全

第一节　一般规定

第二十一条　国家实行网络安全等级保护制度。网络运营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：

（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；

（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；

（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；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第二十二条　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。

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。

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。

第二十三条　网络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。

第二十四条　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。

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。

第二十五条　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。

第二十六条　开展网络安全认证、检测、风险评估等活动，向社会发布（公表）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。

第二十七条　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。

第二十八条　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。

第二十九条　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。

第三十条　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。

第二节　关键信息基础设施的运行安全

第三十一条　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。

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。

第三十二条　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。

第三十三条　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。

第三十四条　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：

（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；

（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；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

（五）法律、行政法规规定的其他义务。

第三十五条　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会同国务院有关部门组织的国家安全审查。

第三十六条　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。

第三十七条　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。

第三十八条　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。

第三十九条　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：

（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；

（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配合能力；

（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；

（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。

第四章　网络信息安全

第四十条　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。

第四十一条　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。

第四十二条　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。

第四十三条　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。

第四十四条　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。

第四十五条　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。

第四十六条　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。

第四十七条　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。

第四十八条　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。

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，并向有关主管部门报告。

第四十九条　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。

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。

第五十条　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。

第五章　监测预警与应急处置

第五十一条　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。

第五十二条　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。

第五十三条　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。

第五十四条　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。

第五十五条　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。

第五十六条　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。

第五十七条　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。

第五十八条　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。

第六章　法律责任

第五十九条　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。

第六十条　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：

（一）设置恶意程序的；

（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；

（三）擅自终止为其产品、服务提供安全维护的。

第六十一条　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。

第六十二条　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。

第六十三条　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。

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。

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。

第六十四条　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。

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。

第六十五条　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。

第六十六条　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。

第六十七条　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。

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。

第六十八条　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、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。

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。

第六十九条　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：

（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；

（二）拒绝、阻碍有关部门依法实施的监督检查的；

（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

第七十条　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。

第七十一条　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。

第七十二条　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。

第七十三条　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。

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。

第七十四条　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。

第七十五条　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。

第七章　附　则

第七十六条　本法下列用语的含义：

（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。

（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。

（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。

（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。

（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。

第七十七条　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。

第七十八条　军事网络的安全保护，由中央军事委员会另行规定。

第七十九条　本法自 2017 年 6 月 1 日起施行。