我国关键信息基础设施安全保护白皮书

中国电子信息产业发展研究院网络安全研究所

赛迪（青岛）区块链研究院

二零二一年五月

目　录

一、关键信息基础设施概述

（一）关键信息基础设施定义

关于“关键信息基础设施”（critical infor- mation infrastructure，简称 CII），《网络安全法》给出的定义，即：“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、公共利益的设施。”CII 最初是由通信信息网络发展而来，信息和电信部门构成了其主要部分。随着网络的应用和普及，CII 不仅仅局限于此，还涵括了电信、计算机、互联网、卫星、光纤等支撑基础设施运行的部分。

（二）范围界定

在我国，《关键信息基础设施安全保护条例（征求意见稿）》对关键信息基础设施（“CII”）的范围进行了界定。关键信息基础设施保护范围界定如下：

1.政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位；

2.电信网、广播电视网、互联网等信息网络，以及提供、和其他大型公共信息网络服务的单位；

3.国防科工、大型装备、化工、食品药品等行业领域科研生产单位；

4.广播电台、电视台、通讯社等新闻单位；

5.其他重点单位。

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。

（三）关键信息基础设施安全保护的重要性

一是关键信息基础设施关乎国家安全和社会稳定。随着信息化的快速普及和发展，关键信息基础设施作为事关国家安全和社会稳定的重要战略资源的地位日益凸显。首先，互联网的飞速发展，使得网络入侵和网络攻击事件频发，严重威胁着关键信息基础设施的正常运转，给国家安全带来极大隐患。其次，关键信息基础设施是恐怖主义和网络攻击的重点对象,各国均将视为网络安全的重点并上升到国家安全的高度。通常认为,关键基础设施或关键信息基础设施是支撑国家安全和公共利益的重要基础设施。同时，国家之间的网络战争威胁日益加剧。信息技术的快速发展极大地开拓了互联网络平台，网络攻击不再仅仅依附于传统的常规战争而存在，已经拓展和波及所有与网络相关的事件和人员，通过技术手段破坏关键信息基础设施从而导致政府机构、通信瘫痪已然成为网络战争的重要手段。基于此，为了更好地应对各

种形式的网络攻击，维护国家安全和社会稳定，应加强对关键信息基础设施的保护。

二是加强关键信息基础设施安全保护是社会持续运转的重要保障。关键信息基础设施为国家机构、各行业正常运转提供必需的产品和服务。关键信息基础设施承载或支撑着各行业关键核心业务，即支撑部门行使职能，对于部门或行业稳定运行具有战略性作用。其次，关键信息基础设施是行业运作体系中被强依赖的关键节点，它所承载的业务对其他部门或行业核心业务有较大关联性影响。对这类关键信息基础设施的攻击所产生的破坏，通过关联的行业、领域逐渐传递，会造成连锁连片的严重后果。且随着国家信息化战略的实施和通信技术的不断升级，关键信息基础设施建设不断提速，信息技术的研发和应用正在催生新的经济增长点，这对于调整经济结构、转变发展方式具有十分重要的作用。因此，社会的持续运转需要大力加强对关键信息基础设施的保护。

三是对关键信息基础设施进行法律保护是顺应国际形势的必要举措。目前各个国家均已建立关键信息基础设施安全保护的相关制度，美、德、英、日等国家通过出台和发布政策、法律、标准等多种措施，构建了国家关键信息基础设施保护体系。各国通过发布或升级监管框架、出台指南、完善机构设置等方式进一步推动关键信息基础设施的安全防护工作落地和具体化，提升工业信息安全防护水平。而针对

新一代信息技术的应用可能面临的信息安全风险，也已有一些国家做出了相关的尝试，如英国政府致力于保护关键基础设施免受针对计算机或通信系统的电子攻击威胁，并建立了由国务大臣负责的国家基础设施保护中心为核心，各基础设施部门具体实施相关职责的关键基础设施保护管理体系。因此，为了提升我国关键信息基础设施防护水平，加强监管，防止安全事件发生，我国须加快对关键信息基础设施相关法律法规细则进行研究制定工作。

四是加强关键信息基础设施安全保护对于公民福祉的保障意义重大。加强关键信息基础设施安全保护的根本是对公民福祉、公民利益的保护。关键信息基础设施运行过程中存储或传输的信息数据大量集中或极其敏感，其中供水、供电、医疗卫生、社会保障等公共服务领域的信息系统、政务网络及网络服务提供者所有和管理的网络及系统中有大量的公民身份信息、金融信息等，这些信息一旦被恶意收集或利用，必将损害公民的利益。其次，基于其他行业对于关键信息基础设施的依赖性，加强关键信息基础设施的保护，可以使得公民的工作、生活等更加便利。国家安全、社会稳定及社会的持续运转等是公民福祉得以保障的前提，故加强关键信息基础设施建设也关乎公民福祉。

二、重点国家和地区关键信息基础设施安全保护的做法与启示

（一）重点国家、地区关键信息基础设施保护措施

1.美国

美国最早对关键基础设施领域的相关系统安全进行关注，现已形成较为完善的关键信息基础设施安全政策和战略，且这些政策和战略随着形势变化而逐步调整强化。

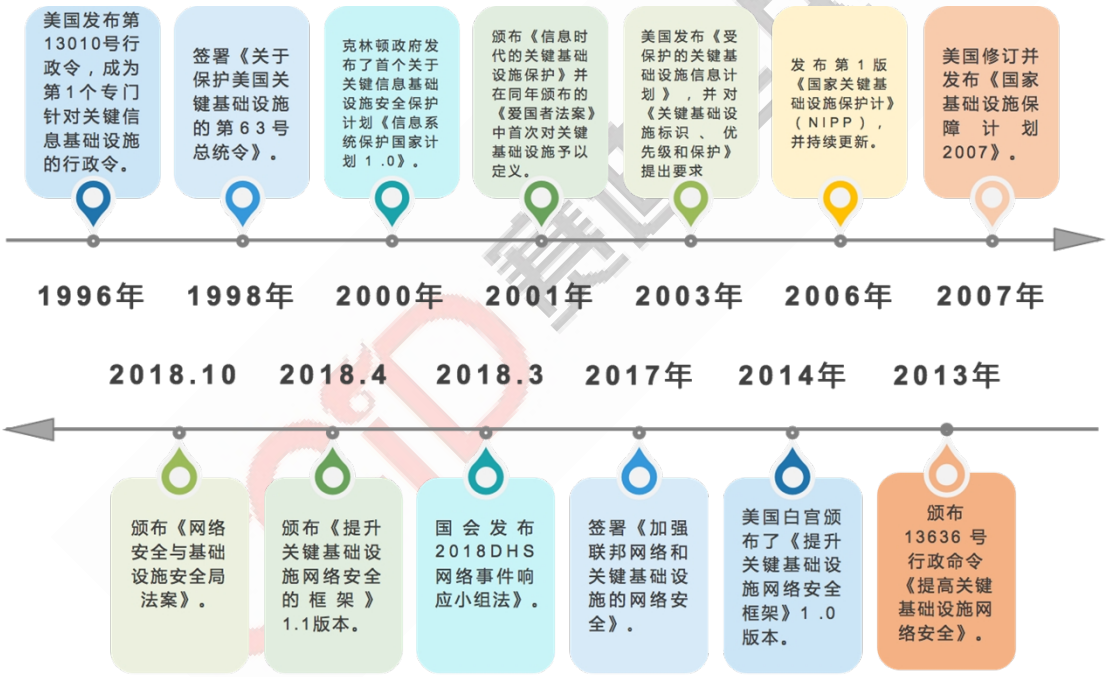

图 2-1 美国关键信息基础设施保护法律汇总

美国关键信息基础设施安全保护计划将风险管理作为保护工作的基础和指针，将保护范畴、责任者与协作方、目标与措施有机连接在一起，构建了与行业实际相适应的保护体系，美国关键信息基础设施保护计划具有以下四个特点：

一是根据行业发展和风险点确定保护重点。针对信息和通信技术发展变化可能对关键基础设施安全保护策略影响，例如云计算的普遍应用、移动计算和移动应用程序的大幅增长、物联网设备以及智能传感器/智能设备快速增长等予以重点关注和应对；**二是依据风险特性建立了多层次的保护工作组织体系。**在充分利用国家级国家关键信息基础设施协调中心（NCC）、信息共享和分析中心（ISAC）基础上，结合行业保障需求分别设立了 IT SCC、IT GCC 等组织，促进安全战略、政策、活动、情报等多维度交流；**三是依托全风险评估方法。**建立与 IT 部门虚拟化、分布式关键基础设施结构相适应的评估体系。在风险管理的维度上，区分政府与企业不同层次，企业通常基于业务目标实施，政府则更关注保障业务的有效性；**四是注重有效性衡量。建立了风险管理措施效果指标体系。**为了有效衡量保护措施实施效果，制定了统一的衡量方案。列举出实现风险管理目标的各项举措及要求，要求各部门成员按照这一衡量方案，每季度报告保护工作进展情况。

2.欧盟

欧盟也较早认识到关键基础设施的网络安全问题，并陆续颁布一系列政策指令，尤其在成员国协调方面强化关键基础设施网络安全防护。

图 2-2 欧盟关键信息基础设施保护法律汇总

在关键信息基础设施保护方面，欧盟提出了制定了行动计划，并从五个方面提出了保护措施：

一是准备和预防层面：鼓励在成员国之间、公共和私营部门之间通过论坛或伙伴关系等实现有效沟通和经验、信息共享。**二是检测和响应方面：**支持发展欧洲信息共享和预警机制。**三是缓解和恢复阶段：**强化欧盟关键信息基础设施（CII）的防御机制，鼓励成员国及企业制定应急预案并进行应急响应和恢复演习。**四是国际合作方面：**确定保证互联网的稳定性和应急能力为欧盟优先发展事项，鼓励开展国际合作。**五是关键基础设施标准方面：**鼓励欧盟及各成员国在信息和通信技术领域内制定具有广泛适用性的标准和方法。

3. 俄罗斯

为应对关键信息基础设施面临的安全威胁，俄罗斯不仅在政策制度、组织架构、法律法规等方面采取措施，还在公私合作方面制定了使用安全关键信息基础设施的规范。

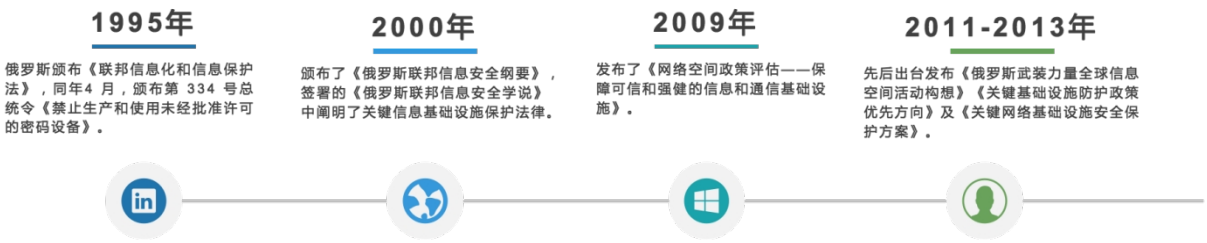

图 2-3 俄罗斯关键信息基础设施保护法律汇总

2009 年俄罗斯的信息安全政策文件中描述的关键部门，主要指科技、国防、通信、司法、应急响应部门等部门。2013 年出台的《俄联邦关键网络基础设施安全》规定：对入侵交通、市政等国家关键部门信息系统的黑客最高可处以 10 年监禁。这事实上是将交通、政府等纳入国家关键网络基础设施。俄罗斯的信息安全战略更多强调在内容层面的管控，非常重视互联网信息传播对传统文化、公民德道和价值观带来的影响，而在基础设施层面，则几乎没有特别具体的描述，只是概括性地表示保护关键信息基础设施。

4. 日本

日本参考了以美国为代表的发达国家在关键信息基础设施安全防护的有关举措，陆续颁布了一系列的相关法律法规，在关键信息基础设施安全防护领域开展了协同性的实践探索。

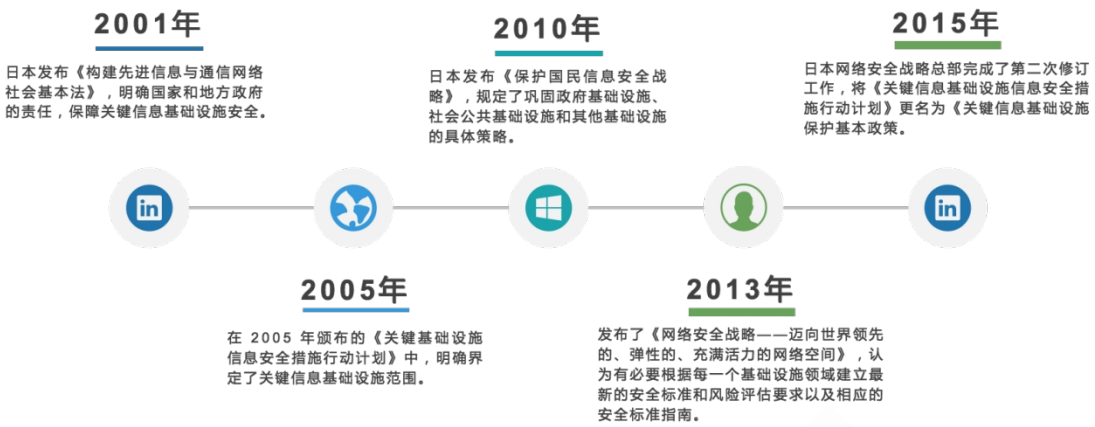

图 2-4 日本关键信息基础设施保护法律汇总

自 20 世纪 90 年代以来，日本持续关注对关键信息基础设施的保护，并已经逐步建立了以政策法律为基础，以组织机构体系建设为重点，以监测预警和信息共享机制为支撑，以技术、人员、资金支持为保障的关键信息基础设施保护制度。日本《关键信息基础设施保护基本政策》中对关键信息基础设施运营者需要采取的措施和国家层面采取的行动，给出了较为详细的描述：

一是持续提升关键信息基础设施安全保护能力。日本内阁秘书处制定安全规则的指导方针，并持续对指导方针进行审查，确认指导方针适合关键信息基础设施运营者网络安全管理的 PDCA 循环，并能够与其他原则配合，使关键信息基础设施保护能力加强。**二是建立信息共享机制。**根据《基本政策》要求，日本内阁秘书处制定了“从关键信息基础设施运营者共享至国家信息安全中心(NISC)的信息”、“信息从 NISC 共享至关键信息基础设施运营者”、“信息共享至 NISC

的事件和原因种类”等政策附件，建立了正常情况下的信息共享机制和 IT 危机下的信息共享机制。**三是通过跨部门演习增强事件响应能力。**特别强调了通过实施跨部门的演习，并在演习中实施有效的培训，增强关键信息基础设施的 IT 中断响应能力，建立完善 IT 中断处置机制。**四是推动运营者和国家两级风险管理。**强调关键信息基础设施经营者应结合本单位业务连续性的要求，制定网络安全风险管理工作目标，制定具体工作计划并在单位内实施，并将应对 IT 故障的措施纳入风险管理工作计划。**五是加强公共宣传、国际合作、标准认证等基础工作。**日本内阁秘书处开展公关，通过简讯、网站、讲座等手段，使公众了解关键信息基础设施保护基本政策，从容应对各种情况，获得最广泛的合作；继续加强国际合作，通过双边、区域间和多边框架，为运营者获取典型案例、最佳实践等；为关键信息基础设施保护发布参考书，系统地安排有关的标准和指南，对国际标准提供应用指南，推动第三方认证和评估等。**六是详述利益相关方应采取的行动。**详细列出了各利益相关方，包括内阁秘书处、关键信息基础设施保护责任部门、信息安全相关部门、危机管理部门、关键信息基础设施运营者、CEPTOAR、CEPTOAR 理事会、关键信息基础设施保护支撑机构和网络空间相关运营者。

（二）国际关键信息基础设施安全保护主要启示

从美国、日本等国家地区关键信息基础设施安全保护的实践来看，关键信息基础设施安全保护重在明确以下4个方面内容：

1.科学界定关键信息基础设施的范围

关键信息基础设施的概念是从关键基础设施发展而来。目前国际上对于关键基础设施的范围界定逐渐趋同，美国提出了16类关键基础设施领域，俄罗斯、日本、欧盟等也提出了相应的关键信息基础设施保护分类方法。我国《中华人民共和国网络安全法》等政策文件也明确了关键信息基础设施的领域范围。但是在实际操作层面，各行业主管部门还应制定本行业、本领域关键信息基础设施具体认定规则。同时各国关键信息基础设施的范围有共性，又有差异，具有原则性和灵活性相结合的特点，要结合本国具体的实际情况，探索科学合理的关键信息基础设施范围界定和认定细则。

2.明晰关键信息基础设施安全保护的目标

国际范围内制定关键信息基础设施安全保护体系时首先要明确本地区关键信息基础设施保护的重点与目标。例如美国提出关键基础设施保护的主要目标在于提高基础设施的安全性和弹性，具体包括安全感知能力、安全控制能力以及应急恢复能力；欧盟关键基础设施保护的目标在于免受大规模网络攻击和中断，重点是预防、安全性和恢复力；日本关键信息基础设施保护的目的是保障关键信息基础设施持

续正常稳定运行，避免由于自然灾害、网络攻击或其他原因造成的 IT 中断事件。我国《网络安全法》提出，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，因此，关键信息基础设施保护应以业务连续性和安全可控性为主要目标。

3.明确关键信息基础设施安全保护的措施方法

从国际方面来看，美国的关键基础设施网络安全保护框架是基于NIST的风险管理框架提出来的，其核心包括识别、保护、检测、响应和恢复5个部分。欧盟提出准备和预防、监测和响应、减灾和恢复、国际合作4个方面行动措施。我国《关键信息基础设施安全保护条例》提出了关键信息基础设施保护的识别认定、安全防护、检测评估、监测预警和应急处置5个基本环节。从各国实践来看，所采取的保护环节和措施都是基于风险控制的动态安全保护周期过程。

4.建立关键信息基础设施保护的组织管理体系

关键信息基础设施保护涉及不同的行业和部门，需要充分调动利益相关方的积极性，明确管理组织机构及其责任。各国在这方面都作了相应的制度设计，例如美国、欧盟等国家地区建立了供应链风险工作组、威胁情报共享中心、紧密联系领域多方会议、网络安全自愿社区等丰富的组织，同时建立了顶层协调机制、信息共享和协同保护制度，明确关键信息基础设施运营者的权责义务、监管部门

的责任以及国际合作机制等。我国相关行业也可借鉴类似模式，组建行业关键信息基础设施保护相关组织，通过定期会议、课题研究、政策研讨等方式强化交流协作，助力保护工作实施。

三、我国关键信息基础设施安全保护现状

（一）法律法规建设加速推进

经过 20 多年的工作推进,我国在网络安全保护法规建设方面取得很大进展,以《网络安全法》为核心的关键信息基础设施安全保护法律保障体系建设正在加速推进。

表 3-1 关键信息基础设施安全保护法律法规汇总

时间	发布主体	法律名称
2006 年	国务院	《国家突发公共事件总体应急预案》
2007 年	国务院	《突发事件应对法》
2013 年	国务院	《突发事件应急预案管理办法》
2016 年	国务院	《网络安全法》
2017 年	国家网信办	《国家网络安全事件应急预案》
2017 年	国家网信办	《关键信息基础设施安全保护条例（征求意见稿）》
2018 年-2019 年	国家网信办	《网络安全等级保护条例（征求意见稿）》、《网络安全漏洞管理规定（征求意见稿）》《网络安全威胁信息发布管理办法（征求意见稿）》等相继向社会公开征求意见
2020 年	国家网信办	《网络安全审查办法》

（二）标准体系逐步完善

为保证关键信息基础设施安全，我国在标准建设方面做了大量的工作。

一是标准化组织建设逐步完善。2002 年 4 月全国信息安全标准化技术委员会（下简称“信安标委”）正式成立，信

安标委直属国家标准化管理委员会，负责全国信息安全标准化工作，统一协调和组织申报信息安全国家标准年度计划项目，组织信息安全领域国家标准的送审、报批、宣贯等工作。关键信息基础设施安全标准化相关的工作由秘书处牵头组织，根据技术内容的不同，由不同的工作组来具体承担。各工作组负责本领域内的标准需求调研、标准制定、标准宣贯、标准实施评价等工作。

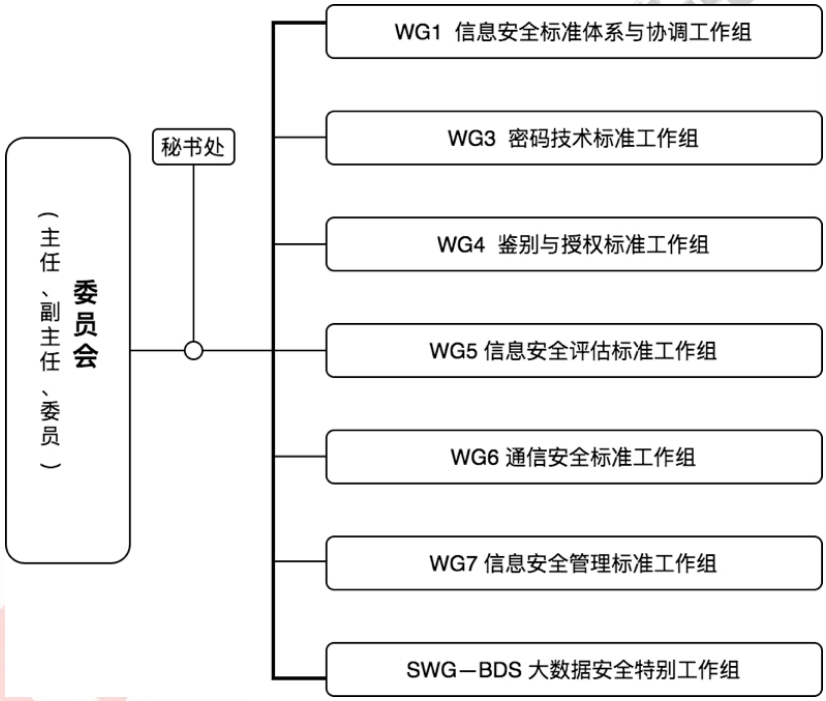

图 3-1 信安标委组织结构

二是从网络安全等级保护标准 1.0 到等保 2.0，我国信息安全保护的基本制度、基本策略和基本方法不断完善。2007 年，《信息安全等级保护管理办法》（公通字[2007]43 号）文件的正式发布，标志着等级保护 1.0 的正式启动，在 2008 年至 2012 年期间陆续发布了等级保护的一些主要标准，构成等级保护 1.0 的标准体系。通过十余年的时间的发展与

实践，成为了我国非涉密信息系统网络安全建设的重要标准。

近年来为适应新技术的发展，解决云计算、物联网、移动互联和工控领域信息系统的等级保护工作的需要，由公安部牵头组织开展了信息技术新领域等级保护重点标准申报国家标准的工作，等级保护正式进入 2.0 时代。等保 2.0 相关国家标准于 2019 年 5 月 10 日正式发布。2019 年 12 月 1 日开始实施。这是我国实行网络安全等级保护制度过程中的一件大事，具有里程碑意义。相较于等保 1.0，等保 2.0 发生了以下主要变化：

表 3-2 等保 1.0 与 2.0 变化对比表

	等保 1.0	等保 2.0
名称	《信息安全技术信息系统安全等级保护基本要求》	《信息安全技术网络安全等级保护基本要求》
定级对象	信息安全等级保护工作直接作用的具体的信息和信息系统。	网络安全等级保护工作的作用对象，主要包括信息系统、基础信息网络、云计算平台、大数据平台、物联网系统、工业控制系统、采用移动互联技术的网络等。
控制措施分类结构	技术和管理两个维度。技术上，划分为物理安全、网络安全、主机安全、应用安全、数据安全；在管理上，划分为安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理。	依旧保留技术和管理两个维度。在技术上，变更为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心；在管理上，调整为安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理。
内容	划分为定级、备案、建设整改、等级测评和监督检查五个规定动作。	变更为五个规定动作+新的安全要求(增加了风险评估、安全监测、通报预

		警、案事件调查、数据防护、灾难备份、应急处置等)。
法律效力	/	《网络安全法》第21条规定“国家实行网络安全等级保护制度,要求网络运营者应当按照网络安全等级保护制度要求,履行安全保护义务”。落实网络安全等级保护制度上升为法律义务。

从等保1.0到2.0，不断完善的等级保护体系在实践中为等保全生命周期提供服务，从定级备案咨询、安全建设整改、等级保护测评、到监督检查改进等均能够提供专业的服务，在辅助企业完成等级保护建设工作的同时，实际提升了系统运营使用单位的信息安全防护能力。

三是标准实施试点有序开展。为验证关键信息基础设施安全保护相关标准内容的合理性和可操作性，信安标委采取了标准实施试点措施。2018年11月8日，信安标委启动了《信息安全技术 关键信息基础设施安全检查评估指南》试点工作。本次试点工作旨在验证评估指南标准制定的科学合理性，为关键信息基础设施安全检查评估工作摸索经验。试点工作选取了包含通信、互联网、交通、能源、金融、电子政务、公共服务等行业在内的12家关键信息基础设施运营者作为标准试点单位，选取中国信息安全测评中心、国家计算机网络与信息安全管理中心等6家第三方测评机构作为检查评估方参与了标准实施试点。试点效果表明，试点机制可

有效验证标准内容是否先进合理和可操作性，有效提高标准的制定质量。

（三）相关研究不断深入

随着我国关键信息基础设施被黑客和相关组织的攻击威胁日益严重,我国在关键信息基础设施安全领域也进行了多方位的研究与探索,包括关键信息基础设施的框架体系、边界识别、风险管控等方面。

一是在框架体系方面，我国相关研究工作人员深入的研究了大数据安全框架体系及其管理模式,建立了基于大数据安全和隐私保护架构的模型,该模型可应用于智慧城市等多种重要场景,通过此模型可以深入摸索城市关键信息基础设施安全框架体系,并对其安全趋势进行评估,为我国关键信息基础设施的安全防御能力奠定良好的基础。

二是在边界识别方面，相关研究工作人员提出了关键信息基础设施安全防护需要识别被纳入保护范围的设施,关键信息基础设施的界定是该领域的重中之重,边界的不明确将会给其安全防护工作带来严重影响,当前有学术研究者通过深入分析关键信息基础设施边界识别所面临的问题及挑战,提出了一种确定关键信息基础设施的边界识别方案。同时,通过研究其他国家关键信息基础设施边界识别的经验,借鉴了边界识别方法。

三是在测量与评估方面，我国相关研究学者基于信息安

全等级保护来研究关键信息基础设施安全防护测量和评估工作,并根据不同行业领域的主要特点,基于信息系统安全评估相关的要求和指南,提出了识别关键信息基础设施属性的风险评估方法,进而实行我国关键信息基础设施的测量和评估工作。

四、我国关键信息基础设施安全保护面临的问题

（一）法律保护范围模糊

虽然《网络安全法》限定了关键信息基础设施的保护范围，但并没有明确指出重要行业和公共服务领域的具体范围和判定标准。同时，《网络安全法》虽然设专节对关键信息基础设施保护进行了规定,但没有进行制定具体的实施要求,大多是方向上的指导和禁止，还需要进一步规定落实的细则和完善的措施。

关于定级对象，根据《信息安全等级保护管理办法》中给的 5 个等级描述都是针对信息系统，也就是说等级保护的对象是信息系统，在《信息系统安全等级保护定级指南》(GB／T 22040—2008)又对信息系统进行了进一步的诠释，对照关键信息基础设施保护，在最新发布的等保 2.0 中，网络安全等级保护工作的作用对象有所增加，包含了信息系统、基础信息网络、云计算平台、大数据平台、物联网系统、工业控制系统、采用移动互联技术的网络等，定级对象的增加为定级方法、保护要求、测评等方面提出了更高的要求，涉及

关键信息基础设施运营的各细分领域及行业的法律法规、保护指南还需加快研究完善。

（二）自主可控能力不足

自主可控能力一向被认为是保障网络安全、信息安全的基本前提。然而，自主可控设备目前还不能完全覆盖我国关键信息基础设施建设和运行管理的要求，我国在引进外国先进技术、加快产业更新换代的同时，也给关键信息基础设施各领域带来许多安全隐患问题。事实上，大量外国信息技术产品已深度渗透至我国的电信、金融、石油、交管等关键网络基础设施,导致我国的经济命脉部分信息实况被外方掌握，系统运行受到控制，甚至存在被境内外敌对势力依令破坏的潜在威胁。当前我国关键信息基础设施的部分设备和部件短期难以摆脱依赖进口的局面，一些信息系统也是由国外企业提供技术服务，且采用的是国外的技术标准，我国对核心元件的控制力较低，缺乏自主可控的技术产品，从长远来看，这对我国的关键信息基础设施的保护而言无疑是致命的安全隐患，只有加大我国自主创新产品的运用才能在日后可能面临的攻击中掌握主动权。

（三）缺乏完善有效的脆弱性评估机制和安全恢复计划

一方面，当前我国大多数关键信息基础设施运营者还没有形成统一的行业安全评估标准，设施脆弱性和风险评估制度也不够完善。仍有部分运营者将工作重点放在事故事件管

理上，甚至只是事故管理，发生事故后再进行整顿、检查，此类防护机制往往会造成重大损失。当前全球范围内的针对CII的蓄意攻击事件频发，例如2015年乌克兰的部分变电站控制系统遭到破坏，造成大面积停电、2017年美国核电站遭受黑客网络攻击等，众多CII安全事件的经验启示我们应当尽快完善风险评估，从而从根源控制，将关口前移。

另一方面，缺乏完善的事后安全恢复计划，当前我国多数关键信息基础设施运营者都未制定完善详尽的事后安全恢复计划，未厘清涉及关键信息基础设施保护过程中的防护流程、未明确指出需要加强保护的重点环节，也无法保障相应评估制度的制定和落实，这为关键信息基础设施保护及快速安全恢复带来了极大的隐患。同时，我国还面临着专业检查评估人员缺少、检查工作耗时多、效率低、检查方法、检查内容不统一的问题。这也为CII脆弱性评估带来了一定程度上的困难。

（四）安全风险监测和预警机制较弱

我国监测和预警机制仍待完善，全国性的风险监测体系还没有建立起来，缺乏完备有效的应急响应措施。目前等级保护2.0提出了在风险监测方面增强了以下措施：“为检验安全防护措施的有效性，发现网络安全风险隐患，运营者制定相应的检测评估制度,确定检测评估的流程及内容等要素，并分析潜在安全风险可能引起的安全事件”。同时在安全预

警方面强调：“运营者制定并实施网络安全监测预警和信息通报制度，针对即将发生或正在发生的网络安全事件或威胁，提前或实时发出安全警示”。目前我国相关行业管理部门以事前控制和预防为核心并根据对关键信息基础设施不同的威胁进行了匹配性工作，但各细分行业内具体的监测与预警标准还未制定，且当前安全预警体制机制还存在各主管机构之间的协调力和联动性欠缺、信息传递机制缺陷，安全风险检测与预警信息共享程度低等问题，安全预警机制改革势在必行。

五、提升我国关键信息基础设施安全保护水平的对策建议

（一）做好基础性研究，制定科学保护框架

目前，虽然《网络安全法》列举了 CII 的保护范围，但是随着互联网信息技术的快速发展，其局限性势必会越来越突显，而且也缺乏相关的认证机制。借鉴国际关键信息基础设施保护经验，我国应做好基础性研究工作，重点开展以下工作：

1.研究我国关键信息基础设施的定义、分类和结构，以及我国CIIP的等级保护框架，研究并不断完善适用于CIIP的定级对象定义及定级对象的确定方法；

2.研究基础信息网络等不同形态定级对象特征研究，研究各细分领域相应的定级方法、基本要求和测评要求；

3.参照基础设施关键性分析方法，结合信息系统所服务的领域，结合基础设施的依赖关系，充分认识定级对象的重要性；研究威胁场景分析方法，分析危害方式；参照风险分析方法，分析和评价危害后果，最终确定各类信息系统、信息网络、平台等对象的安全保护等级。

（二）增强自主创新能力，推动国产技术研发

国家应尽快制定和落实自主创新的政策以建立激励机制，促进关键信息基础设施核心产品的研发，加快人才培养，同时也要加强对关键信息基础设施保护研究的人才和资金支持力度，并建立完整的奖励机制，为技术人员提供强大的物质保障，以此提高我国的关键信息基础设施零部件生产、技术研发的自主可控水平。加快自主开发核心信息技术的进程，必须加快网络认知产品的研发，注重我国自主可控的智慧＋先进技术应用，加强自有网络安全监测、预警技术平台建设。坚持自立创新，开发出我国持有专利的信息技术，并针对我国国情研究出专门的保护技术措施，逐渐减少和降低对国外的依赖，推动 CII 开发建设的国产化进程。

（三）完善检测预警机制，制定应急响应制度与事后恢复计划

早期预警制度是各个国家在关键信息基础设施保护方面的策略之一，也是避免重大网络攻击事件的关键步骤，通过建立完善的监测和应急响应体系，来及时发现安全事件的

发生，并迅速做出反应。为了对即将发生的攻击事件进行快速预警和响应，公共、私营机构应该信息共享共同合作，从而建立应急响应机制，并通过立法来推动该机制的体系化。推动建立应急响应小组协调中心,具体负责协调网络提供商、安全提供商、政府机关与行业协会。积极发挥关键信息基础设施安全事件响应、协调国内关键信息基础设施安全事件响应小组和其他组织的工作、收集安全信息并发布预警通知等职能，以保证事件发生后能及时启动防护措施，并对基础设施进行紧急恢复。

（四）完善安全风险评估认证机制，设立关键信息基础设施专项安全防治体系

完善的安全评估技术可以找出安全威胁来源，并能进行更深入的分析。评估之后，应该设立专门的安全防治体系，针对评估的结果实施正确的管理和技术方案，确保有效地阻止安全威胁，并通过一定的观测手段对可能存在的安全隐患进行监视。可参考借鉴美国启动的著名跨部门持续监控 ISCM 项目，着手建立以实时监控为基础的基于风险的绩效评价，并且这个评价将最终被纳入部门绩效考核。此类机制能够使机构迅速地发现脆弱性并且主动地防范攻击。通过监控与评估发现潜在的影响因子，一旦发现并确认威胁成立，便积极快速激活防护机制，防止或者降低破坏结果扩散。建立安全评估机制同样需要建立动态防护模

式，需要确切的落实，才能真正发挥关键信息基础设施安全监控与防护作用。

（五）相关企业应构建关键信息基础设施的安全管理体系

为保障涉及关键信息基础设施企业的合规化运营，关键信息基础数据的运营者、持有者等必须严格遵循《网络安全法》的相关要求及其下位法的相关规定。除此之外，企业自身也要加强关键信息基础设施保护力度，通过技术与管理手段相结合，构建关键信息基础设施安全管理体系，维护网络空间有序运行。一方面，需综合运用管理、技术、法律、宣传等手段，加强内部自身能力建设，如围绕识别、保护、监测、预警、检测、响应、处置等环节，建立与管理思路配套的技术平台；另一方面，建设分层次防御体系，构建关键信息基础设施外部保护屏障。应从五个方向入手，如坚持自主可控，持续改进风险管理模式，健全跨部门互联网协同安全体系，持续完善配置基线档案管理制度体系形成等保测评问题整改长效机制，关注终端安全管理等。对于终端安全的管理需要更加关注，建立一体化终端安全管理系统，统一策略管控、统一资产管理、统一数据展示。实现国产化、一体化、策略化、强准化、可视化。