ICS 35.020
CCS L70

DB21

辽 宁 省 地 方 标 准

DB 21/T XXXX—XXXX

信息安全技术 网络安全框架

Information security technology-Network security framework

（征求意见稿）

（本草案完成时间：2021-04-12）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

辽宁省市场监督管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中共辽宁省委网络安全和信息化委员会办公室提出并归口。

本文件起草单位：大连软件行业协会、大连交通大学、辽宁省信息中心、大连华信计算机技术股份有限公司、大连奥远电子股份有限公司、大连市计算机学会。

本文件主要起草人：郎庆斌、尹宏、刘宏、于青、胡剑锋、杨万清、杨莉、司丹、孙毅、王小庚。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

本文件归口单位通讯地址：沈阳市和平区光荣街26号甲，联系电话：024-81680033

本文件起草单位通讯地址：大连市高新园区火炬路32号创业大厦A座5层，联系电话：0411-83655207

引　言

0.1 综述

网络安全、网络空间安全，经过几十年的发展，终提升至国家安全战略。经过几十年的发展，特别是进入廿一世纪，迁延至今天，新一代信息技术的逐渐成熟和应用，网络已经成为行业、社会、人群须臾不可离开的工具、支撑技术、生活手段……。皆因此，网络安全威胁与日俱增，常态化痼存。

网络安全生态共生于社会生态，传统文化的浸润，需要建构有效的秩序约束。是故，网络安全框架亦需要基于同样的秩序构建。

0.2 信息安全

信息安全是随着社会进步、科技发展，特别是信息技术的发展不断扩展、延伸和深化的。广义角度，信息安全是保证自然、社会相关信息的状态、信息所依附的管理、技术及安全体系免受威胁、侵害；狭义角度，各类组织的信息资源及其支撑体系、所依附的环境和其它相关因素等不因偶然的或故意的因素，非法或未授权泄露、更改、破坏，及信息内容不被非法控制、识别、篡改。

信息安全应包括传统信息安全（广义和狭义）、非传统信息安全（社会工程学）和个人信息安全。

注：信息资源是各类组织逐步累积的信息、信息系统、生产、服务、人员、信誉等有价值的资产，是由人、信息和信息技术三元素构成的有机整体，是信息化的基本要素。根据信息资源的属性、特征，主要包括信息、软件、硬件、物理、人员及无形资产等。

0.3 网络安全

网络安全，即应用多种信息技术及IT设备、传输线路等，将功能独立的IT系统、各类终端系统互联所构成的虚拟信息平台的安全。

网络安全与信息安全相互交叉、关联、影响和作用，是信息安全聚焦网络的投影。因而，网络安全应基于信息安全角度，整体、系统、统一规划、设计、部署、实施。

0.4 标准结构

本文件基于网络安全框架探讨网络安全框架主要构成要素的主要安全风险，及之于保障网络安全的信息安全构成要素的安全风险，兼之网络安全设计的主要安全考虑。

0.5 实施基准

本文件可作为构建信息安全管理体系的基准，其内容并不一定适应所有网络安全的实际需求，也可能需要本文件未涵盖的内容。宜根据信息安全相关法规、规范和网络安全的实际需求，规划、设计、部署、实施网络安全体系，并与本文件的条款相互引用。

0.6 标准兼容性

本文件可与其它国际、国内信息安全标准及相关标准协调一致，并与这些标准相互配合或相互整合实施和运行。

信息安全技术 网络安全框架

1 范围

本文件提出了网络安全模型和网络安全框架，规定了内容安全、行为安全、网络秩序、数据安全、网络基础平台安全、网络应用安全、信息传输安全、网络安全控制、运行安全、网络运行环境安全、网络服务管理安全和网络安全设计等相关要求。

本文件适用于为网络安全规划、设计和网络安全运行提供指导和通用规则。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

DB21/T 1628 信息安全 个人信息保护规范

中华人民共和国公安部令第33号 计算机信息网络国际联网安全保护管理办法

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络 network

通过连线联结诸多节点并表示相互的关联关系。

3.2

信息网络系统 information network system

应用计算机、通信、多媒体、信息安全等等信息技术和IT设备、传输线路，将功能独立的IT系统、各类终端系统互联，与行为科学、管理科学等共同构成信息网络平台，通过可实现各种功能的软件应用实现资源共享和信息交互。

注：本文件中，“网络”特指“信息网络系统”。

3.3

网络空间 cyberspace

基于网络形成的虚拟的数字社会。

3.4

网络安全 network security

支撑信息网络系统的信息技术和IT设备、传输线路、功能独立的IT系统、各类终端系统，及系统中的数据、信息、资源等，不因偶然的或者恶意的原因受到破坏、更改、泄露。系统正常、可靠地运行，基于网络提供的服务不中断。

注：网络安全定义亦包含信息安全的属性。

3.5

框架 framework

事物的各种构成要素相互关联形成的组织和结构体系。

3.6

网络安全框架 network security framework

与网络安全相关的要素相互关联、作用构成网络安全架构体系。构成要素可依据框架规则形成相应的安全体系。

4 缩略语

下列缩略语适用于本文件。

NGIT：新一代信息技术（New Generation of Information Technology）

ISMS：信息安全管理体系（Information Security Management System）

5 综述

5.1 网络安全模型

5.1.1 模型

网络安全模型如图1所示：

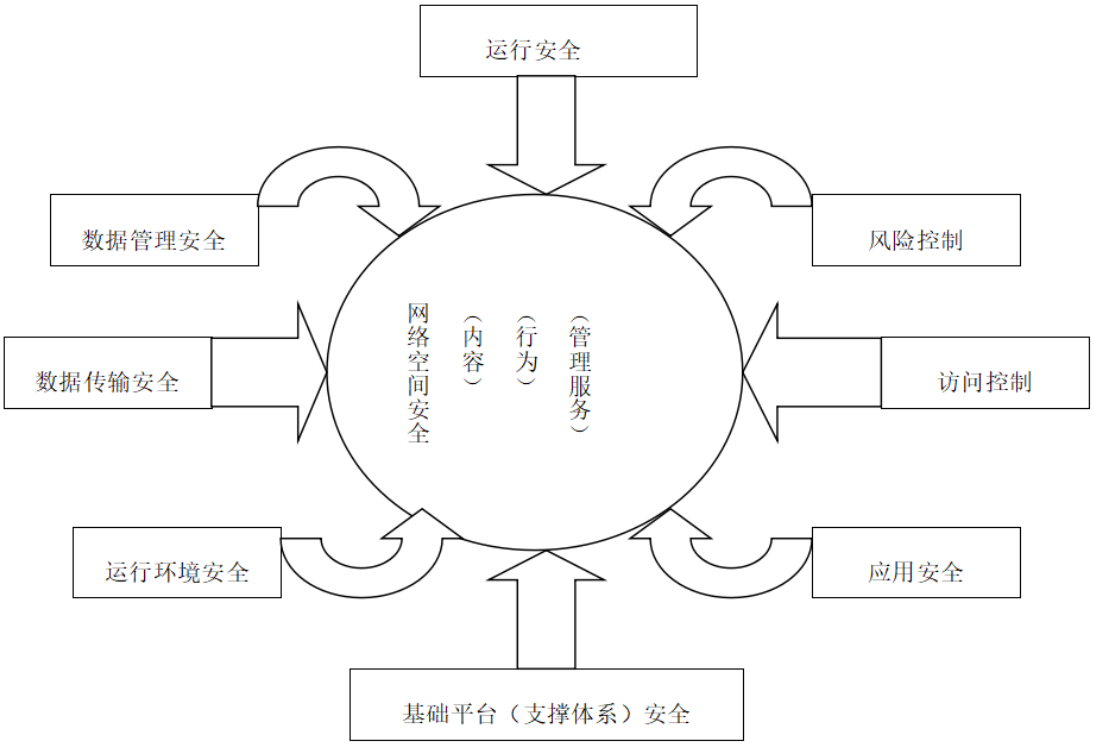

图1 网络安全模型

5.1.2 基点

网络安全模型设计的基点，主要包括：

a) 网络安全的核心应是内容安全；
b) 网络安全的核心要素应是行为（人）、服务（管理）、技术和策略；
c) 网络安全的关键应是风险管理；
d) 在网络构建、运行过程中应建构网络安全保障体系。

5.2 网络安全框架

5.2.1 框架

网络安全框架如图2所示：

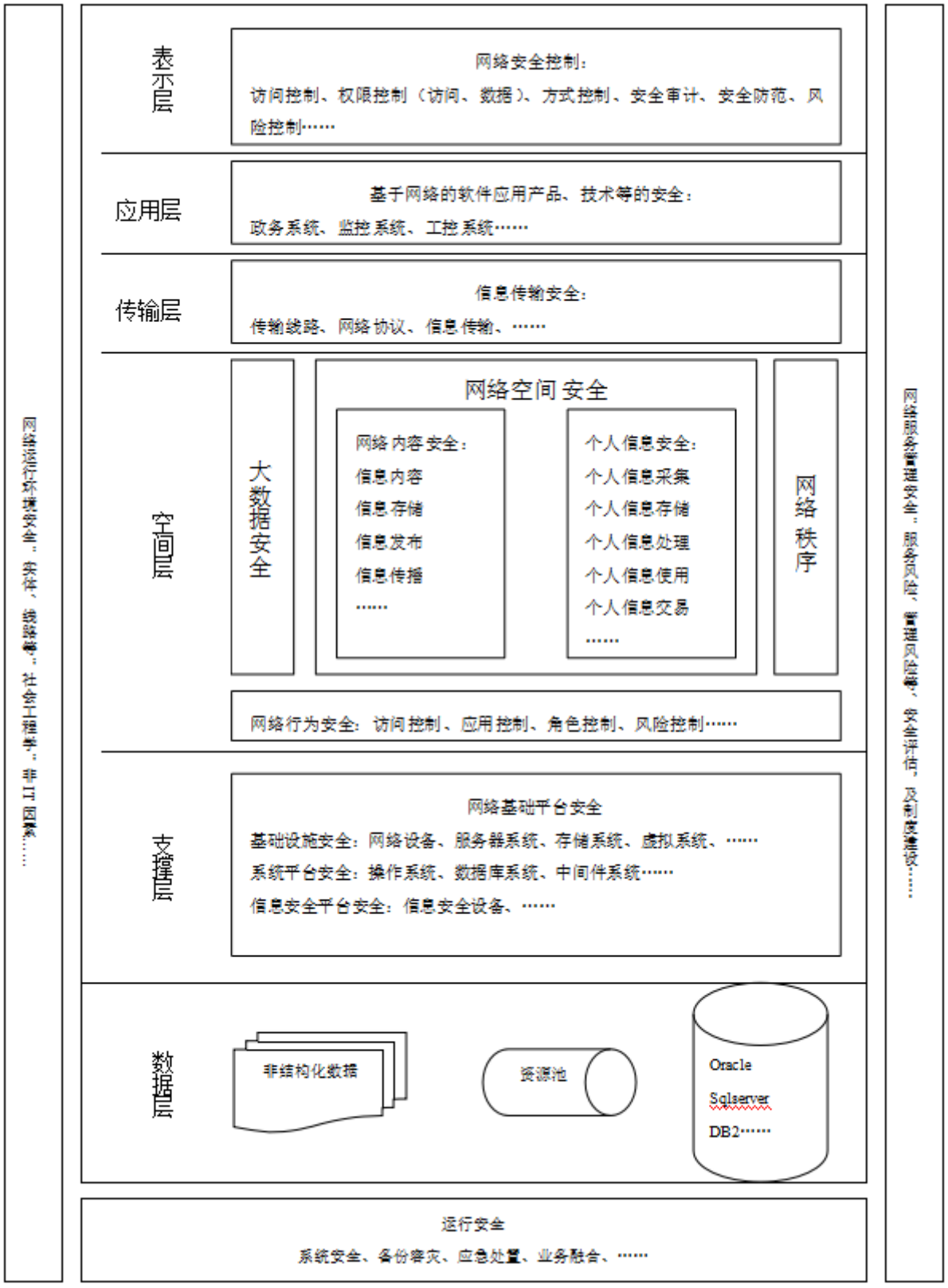
网络运行环境安全：实体、线路等；社会工程学；非IT因素……
表示层
网络安全控制：
访问控制、权限控制（访问、数据）、方式控制、安全审计、安全防范、风险控制……
应用层
基于网络的软件应用产品、技术等的安全：
政务系统、监控系统、工控系统……
传输层
信息传输安全：
传输线路、网络协议、信息传输、……
空间层
大数据安全
网络空间安全
网络内容安全：
信息内容
信息存储
信息发布
信息传播
……
个人信息安全：
个人信息采集
个人信息存储
个人信息处理
个人信息使用
个人信息交易
……
网络秩序
网络行为安全：访问控制、应用控制、角色控制、风险控制……
支撑层
网络基础平台安全
基础设施安全：网络设备、服务器系统、存储系统、虚拟系统、……
系统平台安全：操作系统、数据库系统、中间件系统……
信息安全平台安全：信息安全设备、……
数据层
非结构化数据
资源池
Oracle
Sqlserver
DB2……
运行安全
系统安全、备份容灾、应急处置、业务融合、……
网络服务管理安全：服务风险、管理风险等、安全评估、及制度建设……

图2　网络安全框架

5.2.2 基点

网络安全框架依据网络安全模型形成，其基点主要包括：

a) 网络安全应是信息安全的重要构成，在信息安全总体框架下聚焦网络安全；
b) 空间层应是网络安全模型的核心。空间层涵盖内容、数据（资源）、个人信息、行为、服务（管理）等，并应建构网络秩序；
c) 网络运行环境应是网络运行的基础和保障。应在信息安全总体框架下规划网络运行环境安全；
d) 数据层应是空间层安全的核心。可被网络利用的、以多种形式存在的网络内容（信息的资源）的安全，体现的是信息的主体的权益安全。

5.3 标准设计

本文件设计的基本结构，主要包括：

a) 本文件为网络安全规划、设计、运维提供网络安全特征、安全风险等方面的指导和一般性规则；
b) 本文件的结构，基于网络安全框架展开，以内容安全为核心；
c) 本文件基于一般意义的网络和网络安全设计，可能不适用所有情况。使用者应根据具体情况剪裁、增添；
d) 本文件兼容其它信息安全标准，亦可做为其它信息安全标准的补充或辅助，相互印证。

6 内容安全

6.1 源

网络空间中以各种形态存在的内容，主要源自：

a) 政府通过电子政务或其它方式提供服务的过程中，累积、沉淀的大量与社会公众生产生活息息相关的数据资源。这些数据资源是政府在履行国家机关的职责时获取的公共产品；
b) 公共服务组织在提供各种公共服务的过程中，积累、沉淀的大量数据资源，这些组织包括城市管理、银行、医院、学校等；
c) 各类商业组织在各种商业、商务活动、特别是电子商务中，积累的大量数据资源；
d) 各类企业、经济组织在生产、经营中，累计的大量数据资源等。

6.2 内容类别

网络空间中以各种形态存在的内容，主要包括：

a) 数据：网络行为者的行为数据，如政务应用、商务应用、教育教学应用、网络使用等产生的数据、统计数据、图表等；
b) 信息：基于网络发布的各类信息，如生活信息、招聘信息等；
c) 言论：网络行为者关于国计民生、时局、社会热点、个人诉求等发表的看法和观点；
d) 文献：电子报刊、电子工具书、新闻报道、书目、文献索引等；
e) 个人信息：网络行为者或个人信息主体提供的个人信息主体相关信息等。

6.3 内容形式

网络空间内容的存在形式，主要包括：

a) 文本、图像等；

b） 音频、视频等；
c） 业务、专业领域应用；
d） 信息存储系统等。

6.4 内容特征

网络空间内容的主要特征，主要应包括：
a） 复杂性：网络空间的共享和开放，使网络内容的来源繁杂无序、良莠不齐等；
b） 社会性：网络空间的虚拟化特征，是现实社会的延伸，是网络行为者社会属性的隐性展示；
c） 共享性：网络空间的共享和开放，使网络内容管理分散、无序；
d） 动态性：网络空间的泛化，使网络内容的传递、反馈快速、灵敏；
e） 实时性：网络空间信息流动性特征，使网络内容实现实时传递等。

6.5 安全特征

网络空间内容的安全特征，主要应包括：
a） 社会性：网络空间是现实社会的知识、认知、思维、私欲等的存在载体，因而，网络空间内容映射社会现实和安全；
b） 系统性：网络空间安全是整体的，其构成和相关要素是相互关联影响的。因而，信息安全风险威胁网络构成和网络空间内容；
c） 动态性：网络空间安全的社会属性，使网络空间安全呈现动态变化，网络空间内容的安全随着网络空间安全的动态变化发生改变；
d） 不可追溯性：网络的开放特征，使基于网络的安全事件难以追溯；
e） 灭失性：由于不可追溯性和网络内容管理分散、无序，个人信息失控，可能引发个人信息主体权益不可逆转的灭失。

6.6 安全策略

6.6.1 内容安全

6.6.1.1 信息内容安全

应保护信息内容的真实性、完整性和保密性，避免泄漏、窃听、冒充、诈骗等安全威胁，安全策略主要应包括：
a） 建立信息审核、发布机制；
b） 定义分级、过滤、归类、审计等管理策略；
c） 建立内容监控报警机制等。

6.6.1.2 信息传播安全

网络空间内容的特征，潜藏着网络信息传播的安全隐患。应采取的主要安全策略包括：
a） 应结合信息安全体系建设建立保障网络信息安全传播的安全机制；
b） 应结合信息内容的安全策略，管控行为主体和信息源；
c） 应建立应急事故响应和救济机制，及时处理信息传播过程中的安全事故，修复信息；
d） 应提高网络空间行为者的安全意识，避免安全威胁；
e） 网络空间行为者应遵循相应的秩序规范，避免因滥用网络信息传播自由引发的安全威胁等。

6.6.1.3 信息存储安全

应遵循信息安全相关标准，保证信息存储的安全。

6.6.2 个人信息安全

应遵循DB 21/T 1628，保证个人信息安全。

7 行为安全

7.1 行为分类

网络空间行为可划分为：

a) 基础应用类：包括即时通信、搜索引擎、网络新闻、远程办公、社交应用等；
b) 商务交易类：包括网络购物、网上外卖、网络理财、网上支付、团购、旅行预订等；
c) 网络娱乐类：包括网络游戏、网络文学、网络视频、网络音乐、网络直播等；
d) 公共服务类：包括在线教育、在线政务、在线医疗、网约车等。

7.2 角色

7.2.1 类别

网络空间行为角色，亦应享有民事权利，承担法律责任和民事义务。角色主要应包括：

a) 行为主体：网络空间的行为，如各类应用、创作、个人网站（如微信、微博等）、评论、言论、服务推送等的主导者；
b) 行为参与者：参与部分网络空间的行为，如留言、回复、回帖、讨论、引用等；
c) 行为观察者：并不积极参与网络互动，仅仅浏览、检索、收看、搜索等。

7.2.2 特征

角色特征主要应包括：

a) 角色之间并不发生冲突，行为者可以同时拥有多种不同的角色；
b) 角色并不唯一，是变化的；
c) 社会关系中的角色与网络空间的行为角色存在差异。

7.3 安全特征

网络空间行为的安全特征，主要应包括：

a) 可信性：网络空间行为的可信性，包括基于网络环境的可信性、网络空间行为主体的可信性、网络空间内容可信性和网络空间行为可信性等；
b) 角色变换：角色是多样化的，并不因某种行为而固定。角色变换，对网络空间行为的过程和效果产生影响，亦对社会关系中的现实角色产生影响。

7.4 安全策略

7.4.1 风险管理

应基于网络空间行为的安全特征，识别、分析、评估显性或潜在的风险因素，制定发现应对策略，采取风险管理措施，并监控风险变化。

网络空间行为个体，应提升自我保护意识，评估网络空间行为可能的风险，采取相应的防范措施。

7.4.2 访问控制

应基于网络空间行为的安全特征，定义相应的网络空间内容的访问控制策略，防止未经授权的资源利用。

7.4.3 应用控制

应用控制应是对网络空间行为的控制，包括网络空间的访问、网络空间内容的处理过程和网络空间内容处理结果的行为控制等。应制定相应的安全策略：

a) 应结合访问控制策略，监控、预防网络空间内容的未经授权或恶意访问；
b) 应监控网络空间内容使用过程的行为，控制行为者的合法性、合规性；
c) 应监控、跟踪网络空间内容使用结果的应用和效果，保证行为者的可信性。

7.4.4 角色控制

应结合访问控制策略，定义角色控制策略：

a) 可根据角色属性定义访问控制策略；
b) 可根据角色的不同任务定义相应的控制策略；
c) 应研究角色变换的因素、规律等，采取相应的控制策略；
d) 网络空间行为者应明确角色属性和边界，遵循相应的行为规范，维系网络空间秩序。

8 网络秩序

8.1 法律规则

8.1.1 权利和义务

网络空间行为者应有自由、无障碍使用网络的权利，但应遵守国家相关法律、法规和保密制度，应履行公安部令第33号确定的责任和义务。

8.1.2 法律秩序

网络空间行为者应依法规范网络空间行为，明确网络空间行为的边界，推动相关法律、法规建设完善，构建有效的网络空间法律秩序。

8.2 网络伦理

8.2.1 道德

网络空间行为者在网络空间行为中应遵守普遍认同的道德观念和标准，并在法律秩序约束下展开相应的活动，亦应遵循现实社会的道德规范和法律秩序。

8.2.2 规则

网络行为规则，应是依法规范网络伦理和行为认同的约束标准。在进入网络空间，展开相应活动时，网络空间行为者应严格遵守。

9 数据安全

9.1 综述

数据安全包括数据质量（完整性、可用性等）、数据访问控制、数据交换、数据存储、数据备份和容灾、数据管理，及存储介质等的安全性。

9.2 风险因素

9.2.1 数据质量风险

随着数据类别、数量、形态等的不断增加、变化，数据质量风险日益增大，主要应包括：

a) 数据识别：数据需求、数据目标、数据控制等不明确，数据特点不清晰；
b) 数据分类：数据定义不确切，数据分类不清晰，数据可用性差；
c) 数据冗灾：数据重复、不完整、错误，数据完整性丧失；
d) 数据关系：关联数据间的逻辑关系存在差异，数据一致性出现偏差；
e) 数据标准：数据生命周期内的相关活动缺少标准约束等。

9.2.2 数据访问控制风险

数据访问多样性引发风险，应保证：

a) 访问控制机制选择的安全性、可用性；
b) 访问控制策略定制的可控性、 合理性；
c) 数据访问行为的可控性、可追溯性等。

9.2.3 数据交换风险

数据交换应包括数据通信过程中的数据转发和跨平台、异构数据交换，并保证：

a) 数据的完整性、一致性；
b) 数据合法性、可信赖性；
c) 风险伪装分析、评估；
d) 交换环境的可控性等。

9.2.4 数据存储风险

数据存储的不确定性风险包括：

a) 存储平台的安全性、健壮性；
b) 存储机制的有效性、合理性；
c) 存储网络的可信性；
d) 存储资源的安全控制、安全机制；
e) 访问控制机制的安全性等。

9.2.5 数据管理风险

数据管理的可控性风险包括：

a) 数据管理风险评估的有效性和风险可控性；
b) 数据管理机制的有效性、可靠性；
c) 数据管理能力的强弱；
d) 数据管理的可控性等。

9.3 大数据安全因素

根据大数据的特征，其安全因素主要还应包括：

a) 数据可信性：大量数据的真实性、完整性；
b) 数据泄漏风险：各类数据、个人隐私存在技术风险、管理风险；
c) 数据存储：海量数据存储引发存储架构风险、存储防护风险；
d) 数据攻击：非法行为者利用大数据的攻击风险等。

10 网络基础平台安全

10.1 综述

网络基础平台应是网络运行的支撑体系，构成网络运行的基础环境。网络基础平台安全应是保证网络安全的基础，是信息安全深层防护体系的根本。

10.2 构成

网络基础平台的构成，主要应包括：

a) 网络基础平台：路由设备、网络交换设备、服务器设备等网络基础设施，及网络拓扑结构等；
b) 系统平台：操作系统、数据库系统及网络协议等；
c) 存储平台：集群系统、存储阵列、存储网络等存储设备、虚拟系统等，以及支撑数据存储设施运行的软件平台等；
d) 应用系统平台：支撑系统应用的 Web、DNS、Mail、中间件等服务设施和其它支撑系统应用的软件系统；
e) 信息安全平台：网络安全设施、安全策略、安全机制、安全级别、病毒防护、补丁管理等。

10.3 风险管理

10.3.1 风险识别

应根据网络基础平台的特征，分析、识别网络基础平台的安全威胁、系统漏洞、缺陷等，及安全隐患对系统可能造成的影响、灾难、损失及系统的脆弱性等。

10.3.2 风险分析

根据风险识别的结果，分析风险的来源。风险可能来自基础平台构成要素、技术、工程、管理、环境等，应综合分析风险因素、发生概率、风险感知等，确定风险对网络基础平台的威胁等级。

10.3.3 风险评估

应根据风险分析结果，评估网络基础平台的安全威胁、风险影响、平台要素的脆弱性、安全管理及风险发生的可能性。

10.3.4 风险控制

应制定风险应对计划，控制、跟踪风险变化，并根据风险变化随时调整风险应对策略，并及时识别、分析、评估已发生风险、残余风险和新增风险，以采取适当的应对措施。

10.4 规划设计

10.4.1 要求

规划设计质量决定了网络基础平台的固有质量。应自规划设计阶段保证网络基础平台的安全性、可靠性。

10.4.2 安全因素

规划设计网络基础平台的安全因素，主要应包括：

a) 需求管理：在需求管理中，应明确实际的或可能的需求和需求边界，降低需求变更的风险；
b) 规划合理性：网络基础平台的战略规划、信息安全防御体系、信息安全管理体系等；
c) 设计合理性：网络基础平台的承载能力、整体架构，包括网络拓扑结构、系统平台、存储平台、应用系统平台、安全架构、信息安全平台、数据传输、运行和技术支持、维护和管理等；
d) 功能合理性：网络基础平台的功能设计、构成要素的性能、平台安全性、可靠性等；
e) 配置合理性：配置规划，包括网络基础平台的关联资源、资源分类和部署、资源整合等。

10.5 NGIT

NGIT，如云计算、物联网等，基于泛在的网络平台，突破了传统的网络边界和网络架构，引发新的安全风险：

a) 泛在网络平台的可信性；
b) 新一代网络架构的安全评估；
c) 泛在网络底层互联的信任机制；
d) 泛在网络智能应用的安全风险、隐患和可信性等。

11 网络应用安全

11.1 综述

网络应用是基于网络的各种相关业务应用、控制软件，如电子政务、电子商务、网络监控、工控系统、物联网等。网络应用系统的安全是脆弱的，对网络的威胁是致命的。

11.2 风险管理

11.2.1 要求

应在应用、控制软件开发生命周期全过程建立风险管理框架，识别、分析、评估软件开发过程中的安全风险。

11.2.2 风险管理框架

风险管理框架应包括5个阶段：

a) 需求管理：明确业务需求；
b) 风险识别：识别、分析业务、技术、过程、管理等相关风险；
c) 风险评估：评估风险的威胁、影响等级；
d) 风险控制：风险应对策略；
e) 检测：缺陷修复并检测。

11.2.3 风险识别和分析

风险的识别和分析，主要应包括：

a) 分析、评估业务需求风险；
b) 在软件设计阶段，识别、分析软件架构风险，及软件设计对软件产品的风险影响；
c) 在软件开发过程中，识别、分析系统风险，包括安全机制、系统设计、代码安全等；
d) 识别、分析过程管理风险，包括开发工具、实现技术、项目管理等；
e) 识别、分析开发过程中可能出现的安全隐患等。

11.2.4 风险控制

应在软件开发全生命周期实施风险控制：

a) 应提升软件安全相关知识、技能和经验，以应对可能的风险；
b) 建立检测机制，测试各类应用、控制软件的可靠性、可用性、安全性等；
c) 定义软件开发安全策略、风险应对策略；
d) 建立安全管理规范等。

11.3 应用风险

11.3.1 传统网络应用

应基于传统网络安全边界和网络架构，识别、分析、评估网络应用、控制软件的应用风险和安全因素。

11.3.2 NGIT 应用

应基于NGIT应用，如云计算、移动应用、物联网、智能识别、AI等，建立新的网络应用安全机制，定义风险管理策略：

a) 新一代网络架构应用的安全风险评估；
b) 泛在网络应用的风险识别、评估；
c) 基于新一代信息技术应用的可信性；
d) 基于新一代信息技术应用的风险等级；
e) 建立基于新一代信息技术应用的检测机制；
f) 基于新一代信息技术应用风险的应对策略、安全机制等。

11.4 安全属性

11.4.1 电子政务

电子政务的安全属性，主要应包括：

a) 无边界性：电子政务系统的规模展示出无边界网络特征，其安全特征更加复杂和多样化。但仍存在局部的有边界系统，根据实际的安全需求制定相应的安全策略，作为评估自身安全状态的标准，但放大到全局，则失去了一般性意义；
b) 开放性：电子政务系统的基本特征是服务。政务信息资源的开放性，使电子政务系统作为社会生活、经济发展的开放平台，成为政治安全，国家安全，经济安全、社会安全问题的载体；
c) 文化性：电子政务系统体现出的文化属性是多元的，在这个平台上可以展示形形色色的社会现象、政府形象和政府意志，并因此呈现出文化安全、意识安全；
d) 技术性：信息技术是电子政务系统的支撑和保障，也是政务应用的实现手段。信息技术的应用和扩散，使电子政务系统存在潜在的技术安全，特别是 NGIT 的应用，更增加了安全风险。

11.4.2 物联网

根据物联网的基本架构，物联网的安全属性，主要应包括：

a) 特殊性：物联网的特殊性应主要存在于感知层。感知设备众多、种类丰富，且多样态、发散随机分布，安全控制能力弱；
b) 广泛性：物联网连接物理世界，所承载的资源价值涉及关键业务和核心领域，承载数据安全、网络空间安全、网络安全、IT 环境安全，以至涉及国家、政治、经济的广义信息安全；
c) 泛在性：物联网基于泛在网络，由于特殊性和广泛性，物联节点众多，物联感知信息传输与应用不能适应目前的网络安全架构。

11.4.3 工控系统

工业控制系统（ICS）包括了监控和数据采集（SCADA）系统、分布式控制系统（DCS）、可编程控制器（PLC）等。工控系统与传统IT的安全属性的区别，主要应包括：

a) 由于工业控制系统的特殊属性，系统运行时间、风险管理方式、安全构架、安全目标及性能需求不同，与传统 IT 安全存在差异；
b) 功能安全和系统有效性：ICS 和 IT 系统安全，其功能是类似的，但由于具有不同的风险和系统关注重点，优先级设计存在很大差异；
c) 可用性：ICS 系统要求高可用性，高可靠性和可维护性，特别关注数据的可用性，非预期的系统中断，影响生产是不可接受的；
d) 封闭性：ICS 系统是独立的，安装专用的控制协议，使用专用的基础设施和应用软件。但许多工控系统设计和实施时采用工业标准计算机、操作系统和网络协议，仍易于与公共网络互联，增加了信息安全体系设计的复杂性。

11.4.4 其它

各类网络应用的各自特征不同，安全属性也不同。应量身设计网络应用安全保障体系，采用不同的安全策略，实现网络应用的相对安全。

12 信息传输安全

12.1 综述

网络信息传输通道是脆弱的。信息传输的安全是系统性的，应包括网络基础设施的安全、传输线路的安全、各种网络协议的安全漏洞，及信息传输过程的安全等。

12.2 风险因素

信息传输的安全风险，主要应包括：

a) 网络基础设施：网络基础设施的风险评估参见第 10 章；
b) 网络协议：TCP/IP、UDP 等各种网络协议，及 RIP、BGP、OSPF 等网络底层协议存在的安全漏洞，缺乏相应的安全机制，威胁数据安全、有效传输；
c) 传输线路：包括 UTP、STP、光纤、无线传输媒介等，在信息发送方和接收方之间建立的物理通道，影响信息传输，承载安全隐患；
d) 安全协议：SSL/TLS 等常用信息传输安全协议存在安全漏洞；
e) 公共网络：通过公共网络资源传输信息，存在极大的安全隐患。但利用公网资源建立专用网络，如 VPN，传输信息的技术，也存在着安全隐患；
f) 传输过程：由于承载上述安全隐患，信息在传输过程中，可能存在监听、截取、泄漏、篡改等风险。

12.3 云风险

12.3.1 云

云应是全分布式、泛在的网络架构形式，其特征主要表现为：

a) 云应是基于泛在网络形成的泛化的网络应用服务架构，基于有线、无线、光纤等多种网络形式；
b) 云架构中无主节点，无明确的主、从节点；
c) 云架构可随着泛在网络延伸，无边界，可扩展；
d) 云应是开放的，可共享，灵活方便等。

12.3.2 安全因素

基于云架构的信息传输安全因素，主要应包括：

a) 可控性：基于云架构的特征，信息传输缺少可控性；
b) 可视性：云架构内安全控制机制的差异性，信息传输缺乏可视性；
c) 协调性：云架构主从节点间安全控制机制的不一致，信息传输缺失协调性；
d) 可信性：云架构各节点间可信机制缺乏，信息传输安全性、可靠性控制弱；
e) 数据质量：基于云架构的安全因素，信息传输的完整性、一致性、符合性难以保证等。

注：云架构主从节点应是节点间发生互联访问时临时形成。

13 网络安全控制

13.1 概述

网络安全控制，指代Web应用安全控制，包括访问控制、权限控制、方式控制、配置管理、安全审计、安全防范、风险控制等。

13.2 风险管理

Web应用安全的风险因素，主要包括：

a) 行为能力：多数网络行为者缺乏相应的技术能力，控制使用风险；
b) 设计缺陷：Web 应用实践表明 Web 应用的技术、结构、环境等存在安全隐患；
c) 协议风险：Web 应用涉及的各类协议存在安全漏洞或缺乏安全机制；
d) 可信关系：Web 应用安全访问控制机制的可信关系存在安全风险；
e) 资源安全：Web 应用资源的安全威胁；
f) 平台安全：Web 平台的安全漏洞；
g) 应用安全：Web 应用系统的安全隐患等。

13.3 安全因素

考虑Web应用安全因素，主要包括：

a) 网络行为：网络行为的可信性；
b) 应用场景：开发者对应用场景理解的偏差可能引发风险；
c) 安全策略：Web 应用安全定义的安全策略、安全机制的合理性、有效性；
d) 安全产品、Web 应用安全产品的可靠性、安全性；
e) 匹配差异：Web 应用服务与相应安全模块间的匹配差异等。

13.4 云安全

云计算、物联网等新一代信息技术的应用对Web安全提出了新的安全需求。云架构Web应用的安全因素主要包括：

a) 云架构各节点 Web 应用系统的安全威胁不一致；
b) 云架构下 Web 应用的安全策略；
c) 主从节点 Web 应用安全策略的同步；
d) Web 应用安全与业务连续性等。

14 运行安全

14.1 概述

网络运行安全是网络服务可持续性的保证，应保障网络系统的稳定性、可靠性和安全性。

14.2 运行要素

网络运行的要素，主要应包括：

a) 目标和原则：应明确网络运行和发展的目标，并确定保证网络运行的基本原则；
b) 策略和流程：应定义网络运行管理策略，建立网络运行管理流程；
c) 人员、资源和技术：应确定网络运行相关人员和职责，评估网络运营相关资源和技术管理；
d) 过程模式：应采用 PDCA 模式管控网络运行管理；
e) 跟踪和评估：应跟踪网络运行管理过程并评估能效等。

14.3 安全因素

14.3.1 运行服务

网络运行服务应包括：

a) 服务引入：网络基础平台规划、设计阶段始，宜同时引入网络运行服务者；
b) 过程参与：网络运行服务者宜全程参与网络建设过程；
c) 服务交付：
   1) 运行交付：通过测试、验收和试运行，保证网络安全、可靠、可用和稳定，交付网络运行服务者；
   2) 过程交付：网络建设过程中和过程后所涉及的所有文档、流程、知识、技术、资源等交付网络运行服务者。
d) 运行评估：评估网络运行要素。

14.3.2 运行安全

网络运行的安全因素，主要应包括：

a) 产品：
   1) 网络构成的各种类产品存在的安全漏洞、网络拓扑结构不合理等产生的安全隐患；
   2) 信息安全产品本身设计、质量、功能、部署、安全性等问题产生的安全隐患。
b) 软件：
   1) 系统软件存在的安全漏洞、后门、设计缺陷等产生的安全隐患；
   2) 应用软件设计缺陷、代码级安全风险、后门、功能差异等等产生的安全隐患。
c) 协议：在网络运行中数据传输产生的各类协议安全漏洞；
d) 配置：各类网络相关产品、各类安全产品配置不当引发的安全隐患；
e) ISMS：信息安全管理体系缺失或不完善形成的安全威胁等。

14.4 安全设计

保障网络安全、稳定运行，主要应包括：

a) 评估网络整体安全状况，监控网络运行；
b) 针对网络各个层面的安全隐患，建立 ISMS，定义安全策略，建立完善的安全管理规章；
c) 监控网络安全产品的运行；
d) 建立备份容灾机制，应对灾难预防与恢复；
e) 建立应急处置机制；
f) 信息技术与业务的无缝融合等。

15 网络运行环境安全

15.1 概述

网络运行环境安全是从广义的信息安全角度定义网络安全的环境。广义的信息安全包含了非IT因素的安全威胁。

15.2 环境安全

15.2.1 场地安全

为保证网络运行场地内所有设备的安全、稳定、无故障运行，监控场地的环境、监测并定期检查电源、通风、接地等所有场地设施的工作状态，发现并报告问题和提出变更建议。主要应包括：

a) 电源管理：将电源有效分配到网络系统中不同的设备组件。应考虑电源设备参数对设备的影响，如过压、过流、浪涌、短路等；
b) 等电位管理：设置配电系统、各类电子设备及附属设施、防雷等的接地等电位体，应考虑静电防护、感应雷电可能形成的电磁脉冲和过电压的干扰和毁坏等；
c) 设备管理：网络相关设备的日常运行和管理、可靠性评价；
d) 环境管理：应考虑场地内通风、温度、湿度、灰尘、灯光等的配置；考虑机柜放置与冷却效率和制冷单元热点的关系；以及可能因功能扩大引起的冷却效率问题等；
e) 灾害预防：应考虑物理和自然灾害发生的可能性，制定应急预案等。

15.2.2 线路安全

主要应考虑布线系统管理和维护，主要应包括监控、诊断、分析设备间、弱电井等区域配线设备、线缆、信息插座等设施，及网络通信线路的工作状态和可能的故障状态，发现并报告问题，提出维护建议，保证网络运行的高可靠性和维护的高效率。

15.2.3 监控系统

主要应考虑监控系统管理和维护，主要应包括监控、诊断、分析门禁系统、各类监控设备等的运行状态、参数变化、提示信息等，发现并报告问题，及时变更、维护，保证监控网络的可靠性。

15.3 社会工程学

15.3.1.1 概述

社会工程学是非传统的信息安全，是在人与人的交往中，利用人性的弱点，如本能的反应、好奇心、信任、贪婪等，运用心理学知识，以交谈、欺骗、伤害等手段，获取利益的攻击行为。

15.3.2 特征

社会工程学的特征，主要包括：

a) 社会工程学以“人”为核心，利用人的脆弱性，采用交谈、欺骗、引诱、伪装等方式，攻击人性的弱点，实现期望的目标；
b) 社会工程学基于心理学的基本原理，利用人性与生俱来的信任、贪婪、好奇、本能反应等弱点，让被攻击者顺从攻击者的意愿，满足攻击者的欲望，获取所需利益；
c) 社会工程学的攻击是复杂的，面临的攻击对象千差万别、攻击环境等客观因素复杂多变，可能综合运用多种技巧。在社会工程学攻击中蕴含了各种奇思妙想和灵活构思，以及各种变化的因素等。

15.3.3 攻击形式

社会工程学的攻击，主要包括2种形式：

a) 物理形式：实施攻击的位置，如工作场所、垃圾搜寻、网络环境、电话等；
b) 心理形式：构建陷阱攻击的方式，如说服、友善、恭维、模仿等。

15.3.4 应用形式

实际应用社会工程学，主要包括2种形式：

a) 社会应用：社会工程学的攻击形式可以在社会生活中常见；
b) 网络应用：下载软件捆绑流氓软件、木马、网络钓鱼、间谍软件等，是利用网络实施社会工程学攻击的典型应用。

15.4 非 IT 因素

网络运行环境安全，包括IT管理、技术、知识、专业等之外的政治、社会、人群、非IT专业技能等因素的安全隐患。

16 网络服务管理安全

16.1 概述

网络服务管理是基于网络运行，保障网络安全、可靠、稳定提供的服务管理过程。

16.2 服务形式

根据不同类别的网络需求和业务需求，提供具有不同特点的服务管理：

a) 服务支持：根据不同类别的网络需求和业务需求，采用电话、远程（在线）、现场等方式，提供持续的服务和技术支持，解决网络运行中各种疑难问题；
b) 服务提供：根据不同类别的网络需求和业务需求，定义服务流程，提供相应的、与服务类别相关的服务和技术支持；
c) 服务交付：提供不同类别网络服务的检测、验收和交付，保证该类服务的可靠性、可用性、安全性及可持续改进。

16.3 过程模式

网络服务管理采用PDCA过程模式：

a) P 模式（计划）：明确服务需求和内容，确定服务目标，制定服务计划和服务流程。服务内容应明确网络服务管理对象的质量控制目标；
b) D 模式（执行）：根据实际需求和质量控制目标，整合相关资源，执行网络服务计划；
c) C 模式（检查）：根据服务计划和质量控制目标，检测、检查、分析、评估服务计划执行情况；
d) A 模式（改进）：根据 C 模式的结果，采取相应的改进、完善、预防措施，或肯定计划的执行情况。

16.4 服务风险

网络服务管理过程中的服务风险，主要应包括：

a) 服务需求：服务需求理解差异，或技术需求与业务需求不一致形成安全隐患；
b) 服务责任：有效服务应承担责任和义务的差异化引起的安全隐患；
c) 服务能力：技术能力、知识能力、业务理解能力、实践经验等服务能力的差异引起的风险；
d) 服务可信性：服务提供者的服务综合服务能力等。

16.5 管理风险

网络服务管理过程中的管理风险，主要应包括：

a) 管理方式的可信性；
b) 管理技术的可行性；
c) 配置能力的可控性等。

16.6 新技术风险

云架构、物联网等新一代信息技术产生了新的网络服务管理风险，主要包括：
a) 架构的复杂性引发服务管理的不确定性；
b) 资源的部署方式产生资源的不可控制性；
c) 服务提供者的服务管控能力降低；
d) 服务提供者的能力、知识、管理等的缺陷引发风险等。

16.7 制度建设

应制定网络服务管理的安全策略和完善的安全管理制度，包括人员管理、文档管理、数据管理、设备管理、软件管理、运行管理、机房管理等。

17 网络安全设计

17.1 综述

基于网络安全框架要素的安全规则，应通过充分、有效的风险管理，设计、建构网络安全防御体系和管理体系，定义合理的安全机制和安全策略，保证网络安全。

17.2 原则

网络安全设计的基本原则，主要应包括：
a) 系统性：应采用系统工程的思想、方法，综合、系统、整体地规划、设计网络安全体系，包括网络安全防御和网络安全管理；
b) 均衡性：应基于实际需求和网络运行环境，建立合理的网络安全体系，使其融合安全性、可用性和适用性；
c) 实用性：应基于实际需求和网络运行环境，建立实用、适用的网络安全体系，不应削足适履，亦不应大而无当；
d) 动态性：应根据需求、技术、管理、发展等因素，动态调整网络安全体系，以适应网络环境变化，满足新的安全需求。

17.3 关键因素

建构网络安全体系的关键因素，主要应包括：
a) 组织的发展规划：网络安全体系规划、设计，应考虑组织的实际需要、发展规划和业务需求（包括适度前瞻），并根据组织的管理、业务特征，识别、分析安全需求；
b) IT 发展规划：组织的 IT 发展规划，确定了组织的发展规划所需的 IT 支撑需求，需要根据 IT 发展规划，规划、设计网络安全体系；
c) 风险管理：规划、设计网络安全体系，应充分、有效的识别、分析、评估组织运行中所有相关因素的安全风险源，并制定相应的风险管理策略；

d) 技术趋势：规划、设计网络安全体系，应充分考虑信息安全技术、知识及相关因素的发展趋势和变化，考虑网络安全特征的变化，选择适用的网络安全技术和产品等。

17.4 防护体系

网络安全防护体系结构参见图3，其特征为：

a) 网络安全防护体系是可扩展的三维框架结构，网络安全防御体系维和网络安全管理体系维保证网络安全框架维的相对安全；
b) 如果网络安全框架每一个要素单元均相对满足安全需求，且与网络系统的整体安全配置一致，则网络系统是相对安全的；
c) 网络安全防护体系是一个整体，三维之间是相互关联、相互作用、相互影响的；
d) 在网络安全防护体系中，不应单纯迷信某一安全措施、安全产品等的作用；
e) 建构网络安全防护体系，应考虑信息安全的整体需求及与网络安全的一致性，不应局隅网络安全。

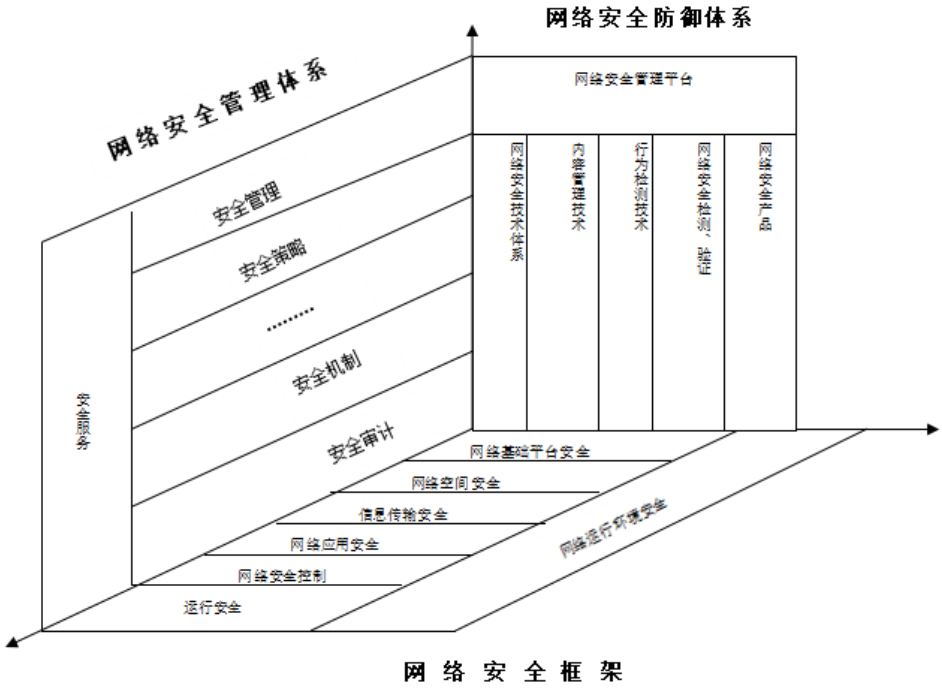

图3 网络安全防护体系

17.5 风险管理

a) 本文件各章之风险管理相关规则，是网络安全框架各要素单元应规范的；
b) 网络安全体系风险管理：
   1) 应综合考虑网络安全框架各要素单元风险管理；
   2) 应整体、系统识别、分析、评估网络系统安全风险；
   3) 应综合考虑信息安全风险与网络安全风险的关联关系。
c) 新一代信息技术的逐渐成熟和应用，网络安全风险应考虑网络的泛化和延展；

d) 应考虑大数据技术、内容多样态丰富等可能潜存的风险异化和行为安全；
e) 应根据隐私，特别是个人信息的特征、价值、权益考虑安全风险等。

参 考 文 献

[1]《中国互联网络发展状况统计报告》