ICS 03.120.10
A01

T/GDCSA

广 东 省 网 络 空 间 安 全 协 会 团 体 标 准

T/GDCSA XXX—2019

基于 GB/T 22239-2019 的医院网络与信息安全保障体系建设指南 第 1 部分：技术要求

Construction guide of network and information security system for hospital based on GB/T 22239-2019—
Part 1:Technical requirement

（征求意见稿）

××××- ××- ××发布　　××××- ××- ××实施

广东省网络空间安全协会　发 布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

T/GDCSA XXXX《基于GB/T 22239-2019的医院网络与信息安全保障体系建设指南》分为3个部分：

——第 1 部分：技术要求；

——第 2 部分：管理要求；

——第 3 部分：软硬件系统符合性功能要求。

本部分为 T/GDCSA XXX 的第 1 部分。

本标准由广东省网络空间安全协会归口。

本标准由广东省网络空间安全协会医疗信息安全专业委员会提出。

本标准主要起草单位：XXXX、XXXX

本标准主要起草人：XXX、XXX、XXX

本标准为首次发布。

引　言

随着我国各级各类医院信息化建设及应用的不断深入发展，为医院服务患者和运营管理带来了极大的便利，大大提高了医疗服务质量和医院的管理水平。与此同时，信息技术的广泛应用也带来了信息安全问题，医院信息安全事件时有发生并见诸报道，不仅严重影响医院的正常运作和管理，而且还威胁着患者的健康和隐私，给社会带来不安定的因素。

2019年5月13日，国家标准新闻发布会上，网络安全等级保护制度2.0标准（以下简称“等保2.0”）正式发布，实施时间为2019年12月1日。等级保护范围涵盖的主要行业有能源、金融、交通、水利、医疗卫生、环境保护、工业制造、市政、电信与互联网、广播电视及政府部门，同时又适应了当前云计算、移动互联、物联网、工业控制和大数据等新技术的应用场景。

在全球网络空间安全面临新挑战、新风险，全国医疗行业信息化面临新任务、新机遇，信息安全领域面临新等保、新管控要求的形势下，广东省网络空间安全协会、广东省医疗行业信息安全标准委员会组织行业专家和安全企业，集专家和安全一线技术人员的聪明才智，采用科学的系统工程方法和问题导向法，遵循《中华人民共和国网络安全法》和等保2.0标准体系，历时四个月时间，联合编制了《医院等保2.0网络与信息安全体系建设指南》，以帮助医疗行业尤其是三级医院根据等保2.0的标准和要求，实施网络信息系统等级保护工程，建立相对完整的医院网络与信息安全保障体系。

基于 GB/T 22239-2019 的医院网络与信息安全保障体系建设指南 第 1 部分：技术要求

1 范围

本部分规定了基于GB/T 22239-2019的医院网络与信息安全保障体系建设的符合性措施、产品功能和性能指标设计及技术实现。

本标准适用于国内三级医院从事医院信息化建设、网络与信息安全管理等相关工作的管理与技术人员学习参考，在建立完整的或升级优化医院网络与信息安全保障体系的时候参照使用，在强化安全管控、监督安全服务、处置应急事件等核心工作环节中增强针对性、操作性，增强安全风险意识和责任意识，提高安全风险辨识能力和责任避险能力。

对于二级及以下医院的同行来说，本标准也具有很好的参考价值，在三级医院要求的基础上对要求项目进行适当裁剪，即可成为二级医院网络与信息安全保障体系的建设指南。同时，在二级医院向三级医院升级的过程中，本标准亦可成为参照标杆物。

本标准同样适合从事医院信息化项目规划建设、医院网络与信息安全保障体系建设和运维工作的IT企业、网络安全公司的售前、售后及运维服务人员学习参考，在提供安全保障、运维服务和应急响应时对照检查并进行自我评价，确保问题处置合理合规，有效减少安全责任事故。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

国卫办规划发〔2018〕4号 全国医院信息化建设标准与规范（试行）

3 术语和定义

下列术语和定义适用于本标准。

3.1

管理视角 Management perspective

从建设方角度看，应采取的网络和信息安全管理策略与措施。

3.2

运维服务视角 Operation and maintenance service perspective

从运维服务方角度看，应采取的网络和信息安全实施策略与措施。

4 缩略语

下列缩略语适用于本标准。

等保1.0：GB/T 22239-2008　信息安全技术 信息系统安全等级保护基本要求。

等保2.0：GB/T 22239-2019　信息安全技术 信息系统安全等级保护基本要求。

5　等保 2.0 标准符合性措施设计

5.1　概述

5.1.1　就医院安全保障体系而言，本标准主要聚焦在等保二级和三级系统的保护能力要求上。

5.1.2　对于二级安全保护，其要求是：“应能够防护免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和处置安全事件，在自身遭到损害后，能够在一段时间内恢复部分功能。”

5.1.3　对于三级安全保护，其要求是：“应能够在统一安全策略下防护免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难，以及其他相当程度的威胁所造成的主要资源损害，能够及时发现、监测攻击行为和处置安全事件，在自身遭到损害后，能够较快恢复绝大部分功能。”

5.1.4　对已实施并通过等保 1.0 定级备案、测评的医院，可以遵循等保 2.0 标准要求进行补齐增强。

5.2　安全通用要求

5.2.1　针对“安全通用要求”之“技术要求”，列出了“物理和环境安全”、“网络和通信安全”、“设备和计算安全”、“应用和数据安全”共 96 项要求，对每项要求在“安全软硬件系统”、“管理者视角”、“运维者视角”三个维度给出了技术解决方案或管理服务的具体措施。具体应符合表 1 的规定。

5.2.2　表 1 中列出的等保 2.0 要求是以三级等保标准提出的要求，对于医院的网络与信息安全保障体系建设而言，当一些 IT 资产的保护等级为二级时，则可以根据等保 2.0 标准降维调整相应的要求。

5.2.3　各方可以按照表 1 中所列的“安全软硬件系统”的建议，利用这些产品所提供的某项功能或多项功能，在编制建设方案的时候将其纳入总体设计中，首先在技术层面解决保障信息安全的产品选型问题。其次，仅有安全产品部署在医院网络上是不够的，更重要的是，如何将安全保障体系建设方和运维方的管理、实施责任落到实处！表 1 最大限度地列举了甲乙双方的责任分工和具体措施，可供甲乙双方在安全管理建章立制工作中参考，也为考核评价运维服务是否达标提供了依据。

5.2.4　对使用本标准的甲方管理者来说，针对每一项等保要求所采取的常规措施包括：通过会议确定“行动计划”，对运维服务方（或自运维）下达任务，待运维服务方执行任务完毕并反馈结果后，根据实际情况做出新的对策，进入下一轮工作。

5.2.5　对使用本标准的运维服务方来说，一方面要配合甲方管理者研究各项具体措施，共同制定“行动计划”，更重要的是执行双方确定的任务，并及时反馈结果给甲方。然后再参与新一轮的决策、执行、检查、反馈环节的工作中。

注：表1中的标准与规范要求是指国卫办规划发〔2018〕4号　全国医院信息化建设标准与规范（试行）中对网络与信息安全保障所提的要求。

表1　通用安全

层面	控制点	等保 2.0 要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全物理环境	物理位置选择	机房场地应选择在具有防震、防风和防雨等能力的建筑内	第三章 基础设施（十二、机房基础）	—	根据水文、气象、地震资料等进行综合论证、申报	实地检查
		机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施	第三章 基础设施（十二、机房基础）	精密空调	实地检查并论证、申报	实地检查,如在顶层或地下室需检测加强防水和防潮措施有效性，并进行记录
	物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员	第三章 基础设施（十二、机房基础）	电子门禁、机房动力环境监控系统	要求配置电子门禁系统，临时来访需审批、登记、录入系统，或者专人陪同并录入系统，视频数据保留 30 天	机房专人值守，定期检查分析出入记录，并进行记录
	防盗窃和防破坏	应将机房设备或主要部件进行固定，并设置明显的不易除去的标记	第三章 基础设施（十二、机房基础）	—	要求机房设备或主要部件固定并标记，设定标签编码规则	定期机房巡检，并进行记录
		应将通信线缆铺设在隐蔽安全处	第三章 基础设施（十二、机房基础）	—	管理制度中明确要求通信线缆铺设在防静电地板下或 PVC 管道中	定期机房巡检，并进行记录
		应设置机房防盗报警系统或设置有专人值守的视频监控系统	第三章 基础设施（十二、机房基础）	防盗报警系统、视频监控系统、机房动力环境监控系统	要求部署防盗报警系统或视频监控系统，对于监控信息需保存 6 个月以上	机房专人值守，定期复查视频记录等，并进行记录告
	防雷击	应将各类机柜、设施和设备等通过接地系统安全接地	第三章 基础设施（十二、机房基础）	建设接地网、机房动力环境监控系统	管理制度中规定范围内的设备必须接地	定期检查接地电阻，并进行记录

表1 通用安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全物理环境	防雷击	应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等	第三章 基础设施（十二、机房基础）	防雷保安器、过压保护装置、机房动力环境监控系统	要求设置防雷保安器或过压保护装置	定期检查防雷设施，并进行记录
	防火	应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火	第三章 基础设施（十二、机房基础）	配置气体灭火自动消防系统、机房动力环境监控系统	要求配置气体灭火自动消防系统，要求定期进行消防演习	定期检查消防系统，出相应报告，配合进行消防演习
		机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料	第三章 基础设施（十二、机房基础）	—	要求机房建设应使用有耐火等级的建筑材料，规定相关范围	定期检查材料的耐火等级、损耗程度，并进行记录
		应对机房划分区域进行管理，区域和区域之间设置隔离防火措施	第三章 基础设施（十二、机房基础）	复合岩棉彩钢板、铯钾防火玻璃等	要求对机房中重要信息或者关键业务系统需要和常规信息系统和设备进行隔离；要求隔断防火设备需采用复合岩棉彩钢板、铯钾防火玻璃等	检查存储重要信息和关键信息系统是否有与普通信息系统进行隔离，隔离方式是否满足要求，并出具分析报告；定期检查隔断材料的耐火等级、损耗程度并进行记录
	防水和防潮	应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透	第三章 基础设施（十二、机房基础）	遮雨板盖	要求采取措施防止雨水通过机房窗户、屋顶和墙壁渗透	定期检查防雨情况，出相应报告
		应采取措施防止机房内水蒸气结露和地下积水的转移与渗透	第三章 基础设施（十二、机房基础）	湿度仪、排气扇、机房动力环境监控系统	要求采取措施防止机房内水蒸气结露和地下积水的转移与渗透	定期检查防水情况和监控系统运行情况，并进行记
		应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警	第三章 基础设施（十二、机房基础）	安装对水敏感的检测仪表或元件、机房动力环境监控系统	要求安装对水敏感的检测仪表或元件；	定期查看仪表，查看设备工作是否正常，并进行记录

表1 通用安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全物理环境	防静电	应安装防静电地板并采用必要的接地防静电措施	第三章 基础设施（十二、机房基础）	防静电地板、构建接地网	要求采用防静电地板、构建接地网	定期测试设备防静电效果，并进行记录
		应采用措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等	第三章 基础设施（十二、机房基础）	静电消除器、防静电手环	要求采用静电消除器、人员在电力实施过程中要求佩戴防静电手环等	定期检查设施损耗程度，并进行记录；抽查检查实施人员是否有按照要求佩戴防静电手环
	温湿度控制	机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内	第三章 基础设施（十二、机房基础）	精密空调、机房动力环境监控系统	要求机房配置精密空调	定期检查空调运行状态，并进行记录
	电力供应	应在机房供电线路上配置稳压器和过电压防护设备	第三章 基础设施（十二、机房基础）	配置稳压器和过电压防护设备、机房动力环境监控系统	要求机房需配置稳压器和过电压防护设备	定期检查设施损耗程度和运行情况，并进行记录
		应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求	第三章 基础设施（十二、机房基础）	UPS、柴油发电机等、机房动力环境监控系统	要求机房需配置UPS、发电机等	定期检查UPS损耗程度、柴油发电机的运行情况，并进行记录
		应设置冗余或并行的电力电缆线路为计算机系统供电	第三章 基础设施（十二、机房基础）	电力电缆线路冗余或并行	要求机柜供电为双电路	定检查电力电缆线路切换是否正常，出相应报告
	电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰	第三章 基础设施（十二、机房基础）	—	要求电源线和通信线缆应隔离铺设，明确最短距离	定期检查临时拉线情况，并进行记录

表1 **通用安全**（续）

层面	控制点	等保 2.0 要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全物理环境	电磁防护	应对关键设备实施电磁屏蔽	第三章 基础设施（十二、机房基础）	屏蔽机柜、空间干扰器	管理制度中规定关键信息范围、关键设备范围，放置于屏蔽机柜中，可增配空间干扰器	定期进行电磁泄露检测，并进行记录
安全通信网络	网络架构	应保证网络设备的业务处理能力满足业务高峰期需要	提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性	关键网络节点双机冗余、网管软件、QoS 监控	应根据组织业务特点制定合理的网络设备性能的评价规范；要求采取措施监控网络设备性能；关键设备实现双机冗余；配件冗余	应检查业务高峰期一段时间内主要网络设备的 CPU 使用率和内存使用率是否满足要求；检查网络设备是否从未出现过因设备性能问题导致的宕机情况；测试设备是否满足业务高峰期需求；按照业务系统服务的重要次序定义带宽分配的优先级，在网络拥堵时优先保障重要主机
		应保证网络各个部分的带宽满足业务高峰期需要	支持冗余技术设计网络拓扑结构，避免关键节点存在单点故障	关键网络节点双机冗余、网管软件、QoS 监控、CDN 网络加速	要求网络进出口和核心网络的流量满足高峰期需求；尽量采用不同运营商网络通信线路，保障网络业务的连续性；对外提供服务的高访问量系统，需要应用网络加速技术，降低网站访问的拥堵和卡顿，提高响应速度	检查各通信链路宽带是否满足高峰期时段的业务流量需要；测试验证网络带宽是否满足业务高峰期需求；分析不同区域对特定内容的访问频度，有针对性的进行 CDN 加速

表1 通用安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全通信网络	网络架构	应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址	网络区域划分	交换机VLAN、SDN技术	定网络区域划分原则；采取VLAN等技术逻辑隔离；能够根据需要对不同网络区域配置合理的访问控制策略	检查是否依据单位部门情况、信息系统重要程度等因素划分不同的网络区域；检查相关网络设备配置信息，验证划分的网络区域是否与划分原则一致
		应避免将重要网络区域部署在网络边界处，重要区域与其他网络区域之间采取可靠的隔离手段	网络区域划分	防火墙、虚拟化防火墙、网闸	要求边界部署防火墙，明确基本的防火墙策略	检查网络拓扑图是否与实际运行环境一样；检查重要网络区域是否部署在网络边界处；检查重要网络区域与其他网络域之间是否采取可靠的技术隔离手段，如网闸、防火墙和设备访问控制列表(ACL）等；业务终端与业务服务器之间建立安全路径；保存有重要业务系统及数据的重要网段不能直接与外部系统连接，需要和其他网段隔离，单独划分区域

表1 **通用安全**（续）

层面	控制点	等保 2.0 要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全通信网络	网络架构	应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性	通信线路、关键网络设备的硬件冗余	关键网络节点双(边界和核心防火墙热备、集群或负载均衡，边界和核心交换机热备）机冗余	要求通信线路采用 2 家不同运营商的网络通信线路、关键网络设备的硬件冗余；并要求定期进行高可用演练测试，保障系统具备高可用能力；网络规划设计时，需要考虑网络设备和通信线路的冗余	检查是否有关键网络设备、安全设备和关键计算设备的硬件冗余(主备或双活）和通信线路冗余；定期对系统相关的关键网络设备和安全设备进行高可用运行状态、配置进行巡检，定期组织高可用演练测试，确保高可用配置正确无误，状态正常，故障时可切换；定期检测主备切换的可用性，确保备机及备用线路可正常使用
	通信传输	应采用校验技术或加解密技术保证通信过程中数据的完整性	(225）虚拟专用网络设备、(226）加密机设备	VPN、加密机、SSH、SSL、MD5、防篡改等	要求业务应用和运维管理的通信过程都采用非对称加密、哈希校验等密码技术，保障数据传输过程安全可靠；检查所选设备是否具有国家相关部门加解密认证证书及其证书有效性，如国密算法、商密算法等	验证密码技术设备或组件能发保证通信过程中的数据的完整性；针对发现的问题提出安全加固建议协助加固；采用的技术包括校验码技术、消息鉴别码、密码校验函数、散列函数、数字签名等技术来校验信息传输和存储的完整性
		应采用密码技术保证通信过程中的保密性	(225）虚拟专用网络设备、(226）加密机设备	VPN、加密机、SSH、SSL、MD5、SSL 证书等	要求通信过程中尽量采用 SSH、HTTPS、SSL 证书、MD5、JS 加密等加密技术，对于应用层传输采用代码层 JS 加密	检查是否在通行过程中应用了加密通信协议；检查通信过程中使用的密码算法，加密强度是否与安全需求相匹配，算法安全性是否足够；出具检查报告和加固建议

表1 **通用安全**（续）

层面	控制点	等保 2.0 要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全通信网络	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	—	可信组件、集中审计系统	要求部署可信组件，针对边界设备进行多维度可信验证，并进行审计	检查是否基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证；检查是否在应用程序的关键执行环节进行动态可信验证；验证当检测到通信设备的可行性收到破坏后是否进行报警；验证结果是否以审计记录的形式送至安全管理中心；出具检查报告和加固建议
	边界防护	应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信	—	防火墙、网闸、交换机 ACL、虚拟化防火墙、无线接入网关	制定基本的防火墙策略，明确指定端口进行跨越边界的网络通信，指定端口配置并启用安全策略	采用技术手段(非法无线网络设备定位、核查设备配置信息等）核查或测试验证是否存在其他未受控端口跨越边界；定期分析防火墙日志；根据业务需求优化防火墙策略；出相应报告
		应能够对非授权设备私自联到内部网络的行为进行检查或限制	（196）网络准入控制设备	网络准入系统、终端管理软件、IP 地址管理软件	要求采用网络准入系统、终端管理软件或 IP 地址管理软件等对私自联到内部网络的行为进行限制或自动检查；制定临时接入(有线、无线）规范和审批流程	核查所有路由器和交换机等相关设备闲置端口是否已关闭；测试是否有非授权内联设备；对合法设备进行安全合规性加固；出相应报告；部分易被接入的网络端口采用地址绑定方式防止地址欺骗；提供网络连接日志；监控流量的异常连接

表1 通用安全（续）

层面	控制点	等保 2.0 要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全区域边界	边界防护	应能够对内部用户非授权联到外部网络的行为进行检查或限制	（196）网络准入控制设备	网络准入系统、终端管理软件、防火墙、IP 地址管理软件	安全要求采用网络准入系统、终端管理软件或 IP 地址管理软件等对私自联到外部网络的行为进行限制或自动检查	定期检查、测试是否有非授权外联设备；对合法设备进行安全合规性加固；出相应报告；禁用内网关键终端的 USB 口；禁用内网关键设备的无线网卡；提供网络连接日志；监控流量的异常连接
		应限制无线网络的使用，保证无线网络通过受控的边界防护设备接入内部网络	—	无线 AC、终端管理软件、移动应用管理系统(MAM)、防火墙等边界防护设备	要求限制无线网络的使用，确保无线网络通过受控的边界防护设备接入内部网络	检查无线网络的部署方式，是否单独组网后再连接到有限网络；检查无限网络是否通过受控的边界防护设备接入到内部的有线网络；出具报告和建议
	访问控制	应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信	(183）网络防火墙	防火墙、网闸、交换机 ACL、虚拟化防火墙、下一代防火墙	要求在网络边界或区域之间根据访问控制策略设置访问控制规则；要求默认禁止不必要的通信，关闭不必要的接口；对访问控制策略进行审批，未经过审批策略不能开通	应核查在网络边界或区域之间是否部署访问控制设备并启用访问控制策略；应核查设备是否关闭不需要的接口，是否存在全允许的策略，最后一条访问控制策略是否为禁止所有网络通信；定期分析访问控制策略表，并优化配置出相应报告；禁用 any to any 允许策略

表1 **通用安全**（续）

层面	控制点	等保 2.0 要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全区域边界	访问控制	应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化	(183)网络防火墙	防火墙、网闸、交换机 ACL、虚拟化防火墙、无线接入网关、下一代防火墙	定期对访问控制策略进行检查和梳理；按照最小权限原则，综合分析业务部门访问需求及安全隐患，优化访问控制列表，在访问需求、安全防护、响应速度三方面达到平衡	应核查是否不存在多余或无效的访问控制策略；应核查不同的访问控制策略之间的逻辑关系及前后排列顺序是否合理；定期分析访问控制规则并优化，出相应报告；设置禁用 135.137-139、445 等高危端口策略；设置访问控制策略颗粒度到端口级
		应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许、拒绝数据包进出；	(183)网络防火墙	防火墙、网闸、交换机 ACL、虚拟化防火墙、无线接入网关、下一代防火墙	根据业务需要制定严格的检查策略，对源地址、目的地址、源端口、目的端口和协议等进行检查，控制地址、端口范围	应核查设备的访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数；应测试验证访问控制策略中设定的相关配置参数是否有效。3.定期分析访问控制规则并优化配置，出相应报告
		应能根据会话状态信息为进出数据流提供明确的允许、拒绝访问的能力	—	防火墙、网闸、交换机 ACL、虚拟化防火墙、无线接入网关、下一代防火墙	要求根据会话状态信息，控制粒度为端口级，对为进出数据流提供明确的允许、拒绝访问的能力；对访问控制策略进行审批，未经过审批策略不能开通	应核查是否采用会话认证等机制为进出数据流提供明确的允许、拒绝访问的能力；应测试验证是否为进出数据流提供明确的允许、拒绝访问的能力；定期分析访问控制规则并优化配置，出相应报告

表1 **通用安全**（续）

层面	控制点	等保 2.0 要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全区域边界	访问控制	应能根据会话状态信息为进出数据流提供明确的允许、拒绝访问的能力	—	防火墙、网闸、交换机 ACL、虚拟化防火墙、无线接入网关、下一代防火墙	要求根据会话状态信息，控制粒度为端口级，对为进出数据流提供明确的允许、拒绝访问的能力；对访问控制策略进行审批，未经过审批策略不能开通	应核查是否采用会话认证等机制为进出数据流提供明确的允许、拒绝访问的能力；应测试验证是否为进出数据流提供明确的允许、拒绝访问的能力；定期分析访问控制规则并优化配置，出相应报告
		应对进出网络的数据流实现基于应用协议和应用内容的访问控制	—	下一代防火墙、虚拟化防火墙、上网行为管理	单位应制定针对网络应用、应用内容及行为的管控规范，并对进出网络的数据流实现基于应用协议和应用内容的访问控制；制定上网行为管理规范，并对违规行为进行检测	应核查是否部署访问控制设备并启用访问控制策略；应测试验证设备访问控制策略是否能够对进出网络的数据流实现基于应用协议和应用内容的访问控制
		应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为	(194)入侵防范设备、(195）入侵检测设备、(198）网络安全入侵防范	APT 预警系统、网络回溯系统、威胁情报检测系统、抗 DDoS、主机入侵检测、EDR 终端检测防护系统	要求在关键网络节点处采用网络入侵检测技术、防止或限制从外部发起的网络攻击行为；定期检查攻击事件报告，安排专职安全管理员对攻击事件进行监控	核查相关系统或组件是否能够检测从外部发起的网络攻击行为；核查相关系统或组件的规则库版本或威胁情报库是否已经更新到最新版本；应核查相关系统或组件的配置信息或安全策略是否能够覆盖网络所有关键节点；应测试验证相关系统或组件的配置信息或安全策略是否有效；定期对安全设备的报警、异常流量和日志进行分析，出相应报告

表1 **通用安全**（续）

层面	控制点	等保 2.0 要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全区域边界	入侵防范	应在关键网络节点处检测和限制从内部发起的网络攻击行为	(194)入侵防范设备、(195)入侵检测设备、(198)网络安全入侵防范	APT 预警系统、网络回溯系统、威胁情报检测系统、抗 DDoS、主机入侵检测、EDR 终端检测防护系统	要求在关键网络节点处采用网络和主机入侵检测技术，检测、防止或限制从内部发起的网络攻击行为；定期检查攻击事件报告，安排专职安全管理员对攻击事件进行监控	应核查相关系统或组件是否能够检测到从内部发起的网络攻击行为；应核查相关系统或组件的规则库版本或威胁情报库是否已经更新到最新版本；应核查相关系统或组件的配置信息或安全策略是否能够覆盖网络所有关键节点；应测试验证相关系统或组件的配置信息或安全策略是否有效；定期对安全设备的报警、异常流量和日志进行分析，出相应报告
		应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击的检测和分析	(194)入侵防范设备、(195)入侵检测设备、(198)网络安全入侵防范	APT 预警系统、网络回溯系统、威胁情报检测系统、抗 DDoS、主机入侵检测、EDR 终端检测防护系统	要求采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击的检测和分析；定期检查攻击事件报告，安排专职安全管理员对攻击事件进行监控；对未知的攻击采用自定义本地沙箱技术进行分析	应核查是否部署相关系统或组件对新型网络攻击进行检测和分析；应测试验证是否对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析；分析攻击事件和报警日志，出具分析报告和防护建议

表1 **通用安全**（续）

层面	控制点	等保 2.0 要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全区域边界	入侵防范	当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警	(194)入侵防范设备、(195）入侵检测设备、(198）网络安全入侵防范	APT 预警系统、网络回溯系统、威胁情报检测系统、抗 DDoS、主机入侵检测、EDR 终端检测防护系统	要求当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警；定期检查攻击事件报告进行，安排专职安全管理员对攻击事件进行监控，组建安全应急小组	应核查相关系统或组件的记录是否包括攻击源 IP、攻击类型、攻击目标、攻击时间等相关内容；应测试验证相关系统或组件的报警策略是否有效；分析攻击事件和报警日志，出具分析报告和防护建议；运维人员对安全告警事件进行响应，及时处理告警事件
	恶意代码防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新	—	防病毒网关、UTM、网络杀毒软件、下一代防火墙	要求全网需部署网络防病毒软件，规定更新频度；在关键网络节点部署带有防恶意代码模块的软硬件系统，规定系统和规则库的更新频率；定期组织安全意识培训；要求在网络边界或重要区域之间单独部署防病毒网关，规定更新频度	应核查在关键网络节点处是否部署防恶意代码产品等技术措施；应核查防恶意代码产品运行是否正常，恶意代码库是否已更新到最新；应测试验证相关系统或组件的安全策略是否有效；定期分析防病毒系统的日志，出具分析报告和防护建议

表1 通用安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全区域边界	恶意代码防范	应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新	(200)主机恶意代码防范	防病毒网关、防火墙、反垃圾邮件网关、下一代防火墙	要求采取反垃圾邮件技术，规定垃圾邮件界定的基本策略；定期组织安全意识培训	核查在关键网络节点处是否部署了防垃圾邮件产品等技术措施；核查防垃圾邮件产品运行是否正常，防垃圾邮件规则库是否已经更新到最新；设定防垃圾邮件规则库更新频率每小时 1 次，并检查是否已经更新到最新；测试验证相关系统或组件的安全策略是否有效；定期出具策略标准报告
	安全审计	应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	(184)网络安全审计、(185)数据库审计	网络审计、数据库审计、日志审计、OS及数据库开启审计功能堡垒机、安全态势感知	要求在网络边界、重要网络节点进行安全审计，采用网络审计技术对网络、数据库、安全设备、操作系统进行审计，日志保留6个月或以上；确定审计范围；确定审计策略；抽查审计报告；提出策略优化要求	应核查是否部署了综合安全审计系统或类似功能的系统平台；应核查安全审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件进行了审计；定期进行综合分析，根据优化要求及时进行整改；出相应报告
		审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	(184)网络安全审计、(185)数据库审计	网络审计、数据库审计、日志审计、OS及数据库开启审计功能堡垒机、安全态势感知	要求审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；定期综合分析审计记录，出具报告

表1 通用安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全区域边界	安全审计	应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	(184)网络安全审计、(185）数据库审计	网络审计、数据库审计、日志审计、OS及数据库开启审计功能堡垒机、安全态势感知	预留专用审计存储容量；制定定期备份策略，删除审计记录需要进行流程审批	应核查是否采取了技术措施对审计记录进行保护；应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略
		应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析	—	网络审计、上网行为管理	要求远程访问采用SSH、SSL等加密协议，规定加密强度策略；要求相关行为日志进行单独的审计和分析；审计系统应能够对远程访问内部服务器的操作行为进行记录，对访问互联网资源的用户行为，如访问非法站点等违规操作进行记录	定期对远程访问的安全性进行测试：对相关的行为审计和数据进行分析；对远程访问和访问互联网的用户行为实施重点、单独审计和数据分析；出具分析报告
	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	—	可信组件、集中审计系统	安全要求针对边界设备进行可信验证，并进行审计	检查是否基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和通信程序等进行可信验证；检查是否在应用程序的关键执行环节进行动态可信验证；验证当检测到边界设备的可行性收到破坏后是否进行报警；验证结果是否以审计记录的形式送至安全管理中心；出检查报告和加固建议

表1 通用安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换	(186)运维审计 、(202)统一身份管理、(203）电子认证服务、(204）用户身份鉴别	堡垒机、准入控制、4A、应用身份标识及权限管理系统、主机防护、基线核查、防火墙	单位应制定所有类型用户相关的账号密码和系统登录安全管理规范；密码必须满足密码复杂度要求，并定期进行更换；要求终端、服务器、网络设备、安全设备、移动终端、客户端、业务应用系统、数据库均需要采用强度适宜的身份鉴别方式进行验证登录；要求终端、服务器、网络设备、安全设备、移动终端、客户端、业务应用系统、数据库均需要采用身份鉴别方式进行验证登录，鉴别信息必须满足密码复杂度要求，并定期更换；要求采购的软硬件系统具有身份鉴别功能、身份标识唯一性、密码复杂度和密码有效期功能	检查相关设备和软件是否满足身份鉴别要求；检查鉴别信息是否满足密码复杂度要求；出具报告；定期更换密码，对不符合项进行安全加固；定期对系统进行弱密码扫描，并提交扫描结果；对系统进行渗透测试，确认系统身份鉴别功能有效性

表1 通用安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	身份鉴别	应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施	(186）运维审计、(202)统一身份管理、(204）用户身份鉴别、(207）主机身份鉴别	堡垒机、准入控制、主机防护、基线核查、应用身份标识及权限管理系统等、4A	要求终端、服务器、网络设备、安全设备、移动终端、客户端、业务应用系统、数据库均需要采用身份鉴别方式进行验证登录；启用或者开发登录失败处理功能和闲时自动结束或者退出会话功能	检查相关设备和软件是否存在登录失败处理功能；登录失败处理策略是否满足要求，并进行优化
		当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听	(186）运维审计、(202)统一身份管理、(204）用户身份鉴别、(207）主机身份鉴别	堡垒机、应用准入系统、应用系统设定、https、vpn、CA认证、4A	要求终端、服务器、网络设备、安全设备、移动终端、客户端、业务应用系统、数据库等系统的运维操作均采用加密方式进行通信；要求采购的软硬件系统具备安全的远程管理功能，通过安全加密协议进行数据传输	检查相关设备和软件的鉴别信息传输是否有进行加密；软硬件系统应启用HTTPS、SSH等安全加密传输协议，禁用Telnet、Ftp等明文传输方式；出具相关报告
		应采用口令、密码技术、生物技术等两种或者两种以上组合的鉴别技术对用户的身份进行鉴别，且其中一种鉴别技术至少应使用密码技术来实现	(186）运维审计、(202)统一身份管理、(204）用户身份鉴别、(207）主机身份鉴别	堡垒机、应用准入系统、CA系统、主机防护、基线核查、4A	要求终端、服务器、网络设备、安全设备、移动终端、客户端、业务应用系统、数据库等均采用双因素认证技术；要求采购的软硬件系统进行身份鉴别时，提供组合身份鉴别方式；软硬件系统本身无法实现组合身份鉴别方式，可通过采用支持双因素认证功能的堡垒机来间接实现组合身份鉴别	检查是否采用双因素认证方式，并包含密码技术，定期更新有关密码；采用两种或者两种以上组合鉴别身份保证安全(CA Key、手机动态认证码、生物识别等

表1 **通用安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	访问控制	应对登录的用户分配账号和权限	（186）运维审计	堡垒机、应用准入系统、CA系统、主机防护、基线核查、4A	要求对于不同用户分配不同的账号和权限进行规定；根据业务按最小授权原则进行账号权限划分	检查是否有按照实际用户需求进行账号的分配；对不符合要求的账号重新分配权限
		应重命名默认账号或修改默认口令	（186）运维审计	堡垒机、应用准入系统、4A、应用系统设定、主机防护、基线核查	应形成系统实施和配置规范，指引运维和建设实施人员在安装、维护系统时，不使用默认账号和默认密码；要求终端、服务器、网络设备、安全设备、移动终端、客户端、业务应用系统、中间件、数据库等默认用户名(如：root、admin、administrator）需要更改或者禁用；要求软硬件系统的默认用户名和口令进行修改或禁用，并且修改后的口令符合复杂度要求	检查是否有按照实际要求修改默认用户名，提出优化建议，修改后的口令是否符合复杂度要求，出具报告

表1 **通用安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	访问控制	应及时删除或停用多余的、过期的账号，避免共享账号的存在	（186）运维审计	堡垒机、应用准入系统、4A、应用系统设定、主机防护、基线核查	应制定所有类型用户相关的账号安全管理规范，并定期对系统账号进行巡检，及时删除或停用多余的、过期的账号，避免共享账号的存在；要求定期检查软硬件的账号口令清单；制定账号审批流程，管理员对账号申请审批；禁止多个用户使用共享账号	定期检查各类软件硬件中是否存在多余、过期账号，并进行清理；询问是否存在多人共用一账号的情况；出具报告
		应授予管理用户所需的最小权限，实现管理用户的权限分离	—	堡垒机、应用准入系统、4A、应用系统设定、主机防护、基线核查	应配备系统管理员、安全管理员、审计管理员；要求对软硬件系统的管理用户进行分级权限的角色控制，不同角色拥有不同的访问权限，并根据最小权限原则仅授予管理用户所需的最小权限，如系统管理员、安全管理员、审计管理员等	优化权限分配策略，出具报告；应检查是否具有系统管理员、安全管理员、审计管理员账号，检查相应账号权限分配是否合理，出具检查报告
		应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则	—	堡垒机、应用准入系统、4A、应用系统设定、主机防护、基线核查	确认授权主体的管理员，分配相应权限账号。制定账号审批流程，对账号申请进行审核	检查是否依据安全策略配置了主题对客体的访问规则；测试是否存在越权行为；定期对账号清单进行检查，确认是否存在未授权账号；出具报告

表1 **通用安全**（续）

层面	控制点	等保 2.0 要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	访问控制	访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级	—	堡垒机、应用准入系统、4A、应用系统设定、主机防护、基线核查	细化访问控制的粒度，访问主体包含的用户或进程；细化访问控制粒度，被访问客体包含的文件或相关数据库表；对运维人员调查提供的访问控制主体、客体进行抽查核实	定期代码审计，提出优化建议，并出相应报告
		应对敏感信息资源设置安全标记，并控制主体对有安全标记信息资源的访问	—	主机防护、加固软件、数据库防护、数据库审计、4A、水印系统、服务器安全加固、敏感数据分级分类及敏感数据标记系统	对软件系统访问的对敏感信息资源设置安全标记；主体对有安全标记信息资源的访问时，采用访问控制手段	定期代码审计，提出优化建议，并出相应报告
	安全审计	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	(186）运维审计、(187）主机安全审计	堡垒机、数据库审计、4A、主机防护、基线核查	要求终端、服务器、网络设备、安全设备、移动终端、客户端、业务应用系统、中间件、数据库等开启自身审计功能，日志保留 6 个月；应用开发商应增加应用系统日志审计功能，并且应覆盖到每个用户，同时对重要安全事件进行审计	检查各类设备和软件是否看起自身审计功能和策略；检查日志保存是否满足 6 个月的需求；提出优化建议；并出具报告；若使用堡垒机和数据库审计等审计产品，则需确认是否审计到每个用户的重要行为

表1 通用安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	安全审计	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	(186）运维审计、(187）主机安全审计	堡垒机、数据库审计、4A、主机防护、基线核查	要求采用安全审计技术，日志保留6个月；确定审计范围；确定审计策略；抽查审计报告	定期核查事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息，提出优化建议，出具报告
		应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	(186）运维审计、(187）主机安全审计	堡垒机、数据库审计、4A、主机防护、基线核查	预留专用审计存储容量；删除审计记录需要进行流程审批；异地备份存储周期应大于6个月	定期检查是否对审计记录进行保护或者异地备份存储。定期审核所有的删除记录行为是否合规，提出优化建议，出具报告
		应对审计进程进行保护，防止未经授权的中断	(186）运维审计、(187）主机安全审计	4A、堡垒机、数据库审计、综合安全审计、主机防护、基线核查	要求具有对审计功能的保护机制，防止审计进程被非法中断	定期核查审计策略，验证通过非审计管理员的其他账号是否可对审计进程进行中断；根据优化要求及时进行整改；出相应报告
	入侵防范	应遵循最小安装的原则，仅安装需要的组件和应用程序	(188）漏洞扫描设备、(199）主机入侵防范	主机防护、加固软件	要求遵循最小安装的原则，制定最小化清单，仅安装需要的组件和应用程序	定期检查，结合实际运行情况调整最小化清单，出相应报告
		应关闭不需要的系统服务、默认共享和高危端口	(199）主机入侵防范	主机防护、加固软件、漏洞扫描、入侵检测、OS加固	只开放必要的系统服务和端口，禁止默认共享和高危端口；梳理对应开放的服务和端口形成表格，定期维护	定期检查，结合实际运行情况调整最小化清单，出相应报告；结合实际运行情况关闭不必要的服务和端口；定期检查默认共享和高危端口调整端口开放，出相应报告

表1 通用安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	入侵防范	应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制	(199)主机入侵防范	主机防护、加固软件、漏洞扫描、入侵检测、OS加固、堡垒机、IP地址管理	要求采用终端准入技术或IP地址管理手段，通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制	定期核查，调整地址范围，提出优化建议，出相应报告
		应提供数据的有效性校验功能，保证通过人机接口输入或通信接口输入的内容符合系统设定要求	(199)主机入侵防范	应用系统设定、WEB 应用防火墙、云WAF	要求系统建设中需要对接口的输入统一进行有效性校验功能，并保存相关设计文档作为验收文档之一；制定应用开发规范、对系统进行代码审计，审核代码审计报告	定期检查接口安全性，并提出优化建议，出具报告；应用系统需要能够对输入数据接口(软件界面的输入框，如用户名密码输入框、查询信息输入框、留言文本框、文件上传点等）进行输入检查，检查输入的数据是否合规，是否能被绕过攻击，通常结合代码审计、渗透测试做检查，也可通过部署WEB应用防火墙进行安全防护
		应能发现存在的已知漏洞，并在经过充分验证评估后，及时修补漏洞	(199)主机入侵防范	主机防护、加固软件、漏洞扫描、入侵检测、补丁管理系统	要求采用漏洞扫描、入侵检测技术发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞	定期扫描，漏洞修复，不能完全修复的提出替代方案，出相应报告；对渗透测试结果评估后，进行修复
		应能检测到对重要节点进行入侵的行为，并在发生严重事件时提供报警	(199)主机入侵防范	主机防护、加固软件、漏洞扫描、入侵检测、补丁管理系统	要求采用入侵检测设备、web应用防火墙设备对重要节点的入侵进行防护，并能提供及时有效的报警	定期检查入侵检测设备的策略是否符合要求；定期对报警信息进行分析；出具报告

表1 通用安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效中断。	(200)主机恶意代码防范	主机防护、加固软件、恶意代码检查软件、可信软件、EDR终端防护	要求安装防恶意代码软件，定期对恶意代码进行检查，及时删除恶意代码，并定期更新恶意代码库。对重大安全预警，要及时更新。	定期检查恶意代码软件是否已更新到最新版本，恶意代码库是否更新到最新；定期进行恶意代码扫描并进行清除
	可信验证	可基于可信根对计算机设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	—	可信服务器、可信组件、CA系统、审计系统、主机可信安全管理平台	要求对计算机设备进行可信验证，并进行审计	检查是否基于可信根对计算机设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证；检查是否在应用程序的关键执行环节进行动态可信验证；验证当检测到计算机设备的可行性收到破坏后是否进行报警；验证结果是否以审计记录的形式送至安全管理中心；出检查报告和加固建议
	数据完整性	应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	(225)虚拟专用网络设备	防火墙、SSl VPN、hash算法、MD5、国密加密机	设定重要数据范围，要求应用系统采用校验码技术或加解密技术保证重要数据在传输过程中的完整性	定期检查，定期修改密钥，优化加密策略，出相应报告；系统重要数据在传输过程中采用完整性校验技术，如使用SSH、HTTPS方式

表1 通用安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	数据完整性	应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	(225)虚拟专用网络设备	hash算法、MD5、国密加密机	设定重要数据范围，要求应用系统采用采用校验码技术或加解密技术保证重要数据在存储过程中的完整性	定期检查，定期修改密钥，优化加密策略,出相应报告；对于系统备份数据进行hash值校验，避免备份数据被修改；对于系统重要配置文件进行完整性校验，如使用tripwire 等工具进行完整性校验
	数据保密性	应采用密码技术保证数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等	(225)虚拟专用网络设备	防火墙、SSl VPN、Ipsec、HTTPS、MD5、国密加密机	规定数据范围，采用加解密技术保证重要数据在传输过程中的保密性	定期检查，定期修改密钥，优化加密策略，出相应报告；系统重要数据在传输过程中采用加密技术，如使用SSH、HTTPS方式
		应采用密码技术保证数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等	—	存储加密软件、数据库加密、数据防泄漏、文档加密、数据库透明加解密网关	规定存储加密的数据范围，采用加解密技术保证重要数据在储存过程中的保密性，要求定期更新密钥	定期检查，定期修改密钥，优化加密策略，出相应报告；系统重要数据加密进行存储，如windows下禁用密码可还原加密；数据库表单内重要数据使用MD5等加密技术加密
	数据备份恢复	应提供重要数据的本地数据备份与恢复功能	—	容灾备份一体机、云灾备系统	规定重要数据范围，提供重要数据的本地数据备份与恢复功能；制定数据备份恢复规范，定期组织进行数据恢复测试	定期检查，优化备份策略，并出相应报告

表1　通用安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	数据备份恢复	应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地	(236)本地数据备份	容灾备份一体机、云灾备系统	规定重要数据范围，提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；制定数据备份恢复规范，定期组织进行数据恢复测试	定期检查，定期分析优化备份策略，并出相应报告
		应提供重要数据处理系统的热冗余，保证系统的高可用性	(236)本地数据备份	容灾备份一体机	规定重要数据范围，提供重要数据处理系统的热冗余，保证系统的高可用性	定期检查，优化热冗余策略，并出相应报告
	剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	—	应用系统设定	制定开发规范，保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	应用系统用户退出后，该用户鉴别信息被清除，如带有敏感信息的cookie信息；进入控制面板->管理工具->本地安全策略->安全选项查看：建议启用“不显示最后的用户名”
		应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	—	应用系统设定	制定开发规范，保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	进入控制面板->管理工具->本地安全策略->安全选项查看：建议启用“关机前清除虚拟内存页面”；硬盘空间被分配给别的系统使用前，进行数据清除
	个人信息保护	应仅采集和保存业务必需的用户个人信息	(205)个人隐私保护	应用系统设定	制定开发规范，仅采集和保存业务必需的用户个人信息	定期代码审计，提出优化建议，并出相应报告

表1 **通用安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	个人信息保护	应禁止未授权访问和使用用户个人信息	(205)个人隐私保护	应用系统设定	制定开发规范，禁止未授权访问和使用用户个人信息	定期代码审计，提出优化建议，并出相应报告
安全管理中心	系统管理	应对系统管理员身份鉴别，只允许通过其特定命令或系统界面进行系统管理操作，并对这些操作进行审计	—	堡垒机、SOC、4A	要求设置权限独立的系统管理员，制定权限分割细化表，要求采用堡垒机实现4A认证，加强对系统管理员及其权限控制管理，通过堡垒机对操作行为进行审计和记录	定期对管理员的操作日志进行综合分析收集，提出优化建议，出具报告
		应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的日常处理、数据和设备的数据备份与恢复等	—	堡垒机、SOC、4A	要求设置权限独立的系统管理员，其有权对系统资源及其运行规范制定详细的流程设计和配置方案，并进行严格审核	按照流程设计和配置方案要求，严格执行对系统资源和运行配置、控制管路等操作，内部审计相关操作行为是否合规，提出优化建议并出具报告
	审计管理	应对审计管理员进行身份鉴别，只允许通过其特定命令或系统界面进行审计操作，并对这些操作进行审计	—	堡垒机、SOC、4A	要求设立单独的审计管理员并规定其职责，要求部署堡垒机实现4A认证，要求设定可执行的特定命令集，要求审计管理员需要通过特定的界面进行审计管理操作，操作时的各种行为应进行审计和记录	定期综合分析各种审计类记录，提出优化建议，并出具报告

表1 通用安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全管理中心	审计管理	应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等	—	堡垒机、SOC、4A	要求审计管理员需定期对审各类审计记录进行汇总和分析	定期综合分析各种审计类记录，提出优化建议，并出具报告
	安全管理	应对安全管理员进行身份鉴别，只允许通过其特定命令或系统界面进行安全管理操作，并对这些操作进行审计	—	堡垒机、SOC、4A	要求设立单独的安全管理员并规定其职责，要求部署堡垒机实现4A认证，安全管理员需要通过特定的界面进行安全管理操作，操作时的各种行为应进行审计和记录	定期检查系统审计记录，提出优化建议，并出具报告
		应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体和客体进行统一的安全标记，对主体进行授权、配置可信验证策略	—	堡垒机、SOC、4A	要求配置权限独立的安全管理员，要求制定统一的配置策略表，对系统中的安全策略进行配置，包括安全参数的设置，主体和客体进行统一的安全标记，对主体进行授权、配置可信验证策略	定期检查配置策略，提出优化建议，并出具报告

表1 **通用安全**（续）

层面	控制点	等保 2.0 要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全管理中心	集中管控	应划分特定的管理区域，对分布在网络中的安全设备和安全组件进行管控	—	VLAN、防火墙、堡垒机	要求划分特定的安全运维管理区，并增强对此区域自身的安全防护，建议部署堡垒机等设备对网络中的安全设备和安全组件进行管理	定期查看安全管理区域划分情况，并根据实际情况微调优化；定期分析分域策略和该域自身安全保障策略，出具报告；将安全设备统一接入带外管理域进行管理
		应能够建议一条安全传输路径，对分布在网络中的安全设备和安全组件进行管理	—	VPN、加密机、SSH、SSL	要求采用加密传输路径(https、vpn、ssh)对网络中的安全设备和安全组件进行管理	查看传输路径是否安全加密；定期更新密码；定期分析优化并出具报告；将安全设备统一接入带外管理域进行管理
		应对网络链路、安全设备、网络设备和服务器等的运行状态进行集中监测	—	网络监测设备、网管软件、终端检测	要求采用集中监测平台，收集网络链路、安全设备、网络设备和服务器等的监测数据，进行多维度集中监测分析和管理	定期综合分析各类监测设备的日志，出具分析结论和整改调优建议，每月形成总结报告
		应对分散在各个设备的上的审计的数据进行收集汇总和集中分析，并保证审计记录留存的时间符合法律法规的要求	—	日志审计系统、SOC、安全态势感知	要求采用综合日志审计系统对网络中各类设备日志进行统一收集、管理和分析，并保存 6 个月以上	定期查看是否对各设备上的审计记录进行集中并审计，同时查看审计记录是否保存 6 个月以上，提出优化建议，并出具报告

表1 通用安全（续）

层面	控制点	等保 2.0 要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全管理中心	集中管控	应对安全策略、恶意代码、补丁升级等安全事项进行统一管理	—	补丁管理系统、安全态势感知、SOC、EDR 终端防护	要求建立统一的威胁管理平台，联动范围包括主机、网络安全防护和包括统一联动的安全策略，统一的恶意代码库、补丁升级等，安排专人进行统一管理	定期核查相关安全事项有进行统一管理，提出优化建议，并出具报告
		应能对网络中发生的各类安全事件进行识别、报警和分析	—	态势感知系统、安全管理系统、安全大数据分析平台	应建立安全应急管理中心，对网络流量进行抓包分析，展现安全事件及态势，对重要数据设置安全阈值并实时告警	定期检查分析安全事件报警记录，提出整改建议，出具报告

5.3 安全扩展要求

5.3.1 概述

等保2.0在“安全扩展要求”中将“云计算安全”、“移动互联安全”、“物联网安全”、“工控系统安全”分别提出了要求。在各扩展安全类别中，又将扩展要求分为包括（或少于）以下7个部分：即安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全建设管理和安全运维管理。附录A至附录D分别给出了相应的等保2.0要求，同样对每项要求在“安全软硬件系统”、“管理者视角”、“运维者视角”三个维度给出了技术解决方案或管理服务的具体措施。

5.3.2 云计算安全

针对医院自建或租赁医疗云计算中心的项目建设需求，从“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”、“安全建设管理”和“安全运维管理”等7个方面，对照等保2.0的要求提出了共计46项对策措施。具体应符合附录A的规定。

5.3.3 移动互联安全

针对医院移动互联网应用项目的建设需求，从“安全物理环境”、“安全区域边界”、“安全计算环境”、“安全建设管理”和“安全运维管理”等5个方面，对照等保2.0的要求提出了共计19项对策措施。具体应附录B的规定。

5.3.4 物联网安全

针对医院物联网项目的建设需求，从“安全物理环境”、“安全区域边界”、“安全计算环境”和“安全运维管理”等4个方面，对照等保2.0的要求提出了共计20项对策措施。具体应符合附录C的规定。

5.3.5 工控系统安全

针对医院内部的工控系统项目建设需求，从“安全物理环境”、“安全通信网络”、“安全区域边界”、“安全计算环境”和“安全建设管理”等5个方面，对照等保2.0的要求提出了共计21项对策措施。具体应符合附录D的规定。

在《全国医院信息化建设标准与规范（试行）》中，暂未涉及工控系统的安全要求，故附录D中“标准与规范要求”项没有列出具体要求。

6 产品功能和性能指标设计

6.1 医院客户在选择网络和信息安全硬件设备、软件系统的时候，需要考虑软硬件系统产品的重要指标包括功能和性能两方面。

6.2 医院建设方在利用本标准所列出的安全软硬件系统产品功能和性能指标（详见附录 E）的时候，应结合医院实际需求，为这些功能与性能指标赋值（确定具体参数），以便采购和集成到合适的产品。

7 技术实现

为了达到等保2.0标准要求，在附录E中，将建议采用的安全软硬件系统（产品）列在表格之中，供相关人士参考利用。

使用者在采纳这些技术建议时，应充分考虑医院网络的多样性因素，在“物理环境”、“网络通信”、“区域边界”、“设备计算”、“应用数据”、“安管中心”等层面，按照“安全域划分”的网络拓扑结构配置合理的安全软硬件系统（产品），争取用更少的投入、更科学的配置达到等保2.0的总体安全保障要求。

附 录 A
（规范性附录）
云计算安全

云计算安全应符合表A.1的规定。

注：表A.1中的标准与规范要求是指国卫办规划发〔2018〕4号 全国医院信息化建设标准与规范（试行）中对网络与信息安全保障所提的要求。

表A.1 云计算安全

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全物理环境	基础设施位置	应保证云计算基础设施位于中国境内	—	—	云计算关键业务和数据的物理设备位于中国境内	—
安全通信网络	网络架构	应保证云计算平台不承载高于其安全保护等级的业务应用系统	—	—	甲方管理人员应具有相关网络安全意识，保证云计算平台不承载高于其安全保护等级的业务应用系统，如云计算二级平台不得承载三级业务系统；要求云计算运营商提供的云平台，通过等级保护测评，并提供相应的报告；云计算平台需对业务应用系统作备案登记，登记表中明确安全等级	按等保标准自查自测，保证甲方人员租赁或自建的云计算平台不承载高于其安全保护等级的业务应用系统；私有云建设，根据信息系统等保定级情况设计云平台，确保云平台的安全等级不低于信息系统的等级保护要求
		应实现不同云服务客户虚拟网络之间的隔离	（252）云计算安全；（209）虚拟化安全防护	虚拟化防火墙、VPC	采购虚拟化防火墙设备，实现不同云服务客户虚拟网络之间的隔离，保障云平台内部东西向流量的安全防护	在虚拟化防火墙系统上配置相关的安全防护策略，实现不同租户之间的虚拟网络的隔离

表A.1　**云计算安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全通信网络	网络架构	应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力	(252)云计算安全	安全资源池（南北向防护）、云防火墙、IPS	采购网络管理平台、安全管理平台、云平台自身的网络拓扑自动更新功能，绘制与当前运行情况相符的虚拟化网络拓扑；要求云计算运营商的云平台可提供安全防护能力，如访问控制功能和入侵防范等	通过网络管理平台、安全管理平台、云平台自身的网络拓扑自动更新功能，绘制与当前运行情况相符的虚拟化网络拓扑，核对绘制的拓扑是否与当前网络拓扑相符，如有必要，进行手动优化，向甲方人员汇报相关工作；私有云建设可采用具备一虚多的安全硬件、独立安全资源池、云平台自带安全服务等多种方式实现
		应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略	(252)云计算安全	安全资源池（流量编排，安全能力按需提供）、云控制台	要求云计算运营商的云平台可提供对资源、访问控制策略、安全组件等的自主设置功能，如云管理控制台	结合现有或即将采购的云安全能力，采用多租户配置模式，保障甲方云服务业务安全策略设置的合理性，如自定义访问路径、选择安全组件等相关能力；基于SDN构建安全服务链或云平台基于安全服务的编排为云服务客户构建自主安全策略配置能力

表A.1　云计算安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全通信网络	网络架构	应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务	(252)云计算安全	云平台提供对外开放接口	要求云平台可提供对外开放接口，接入第三方安全产品，如云安全市场	依据甲方人员在云平台挂载的业务系统等级保护相关要求，推荐甲方采购相关的安全功能组件，通过相关组件实现业务系统在云端的安全防护；云平台设计开放API,允许第三方安全产品按标准进行对接，由云平台统一提供安全服务
安全区域边界	访问控制	应在虚拟化网络边界部署访问控制机制，并设置访问控制规则	(209)虚拟化安全防护	虚拟化防火墙	要求对虚拟化资源设置网络边界，并设置相应规则	通过防火墙配置相关的网络边界访问控制策略，实现虚拟化边界防护
		应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则	(209)虚拟化安全防护	虚拟化防火墙	应在不同等级(如二级系统和三级系统）网络区域边界部署访问控制机制，完善访问控制规则	应在不同等级(如二级系统和三级系统）网络区域边界部署访问控制机制，完善访问控制规则
	入侵防范	应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等	(252)云计算安全	虚拟化防火墙、安全资源池、抗DDOS、云WAF、IPS、态势感知、主机入侵防御	安全资源池应包含入侵防御组件，为云服务客户提供自身业务系统对外网络攻击行为的检测、记录攻击行为、攻击时间、攻击流量的功能	基于入侵防御组件，为用户提供自身业务系统对外攻击行为的检测、记录攻击行为、攻击时间、攻击流量等工作，有重大攻击事件及时通知用户，做好处置工作

表A.1 **云计算安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全区域边界	入侵防范	应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等	(252)云计算安全	虚拟化防火墙、安全资源池、抗DDOS、云WAF、IPS、态势感知、主机入侵防御	安全资源池应包含入侵防御组件，为云服务客户提供外部网络对自己业务系统的网络攻击行为的检测、记录攻击行为、攻击时间、攻击流量的功能	安全资源池应包含入侵防御组件，为云服务客户提供外部网络对自己业务系统的网络攻击行为的检测、记录攻击行为、攻击时间、攻击流量的功能
		应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量	(252)云计算安全	虚拟化防火墙、安全资源池、抗DDOS、云WAF、IPS、态势感知、主机入侵防御	安全组件应提供检测虚拟机与宿主机、虚拟机与虚拟机之间的异常流量功能	为用户提供检测虚拟机与宿主机、虚拟机与虚拟机之间的异常流量的安全服务，有异常攻击及时汇报和处置。
		应在检测到网络攻击行为、异常流量情况时进行告警	(252)云计算安全	虚拟化防火墙、安全资源池、抗DDOS、云WAF、IPS、态势感知、主机入侵防御	安全组件应提供在检测到网络攻击行为、异常流量情况时进行告警的功能	发现网络攻击行为、异常流量情况时及时汇报，做好处置工作
	安全审计	应对云服务商和云服务客户远程管理时执行特权命令进行审计，至少包括虚拟机删除、虚拟机重启	十五、数据中心安全(五十六）安全审计设备	—	云平台自身应具备对云服务商和云服务客户远程管理时执行特权命令进行审计，云服务客户执行特权命令时应当可被审计	基于云平台提供的审计功能，审计远程管理时执行的特权命令，并定期向甲方汇报相关情况；云平台远程运维应通过堡垒机，以实现特权命令操作、虚拟机删除、关机、重启等行为的管控与审计

表A.1 **云计算安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全区域边界	安全审计	应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计	十五、数据中心安全（五十六）安全审计设备	—	云平台自身应提供相关功能，应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计	定期审计云服务商对甲方云服务系统和数据的操作行为，定期向甲方汇报相关情况；云服务客户自主掌控系统和数据的密钥及访问权限，如果需要云服务商操作及运维，应通过云服务客户的云堡垒机进行访问，以保证云服务客户可做行为审计
安全计算环境	身份鉴别	当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制	(202)统一身份管理	—	当远程管理云计算平台中设备时，管理终端和云计算平台之间应实现双向身份验证	—
	访问控制	应保证当虚拟机迁移时，访问控制策略随其迁移	(252)云计算安全	虚拟化防火墙、主机安全防护软件	采购的虚拟化防火墙访问控制策略必须支持随虚拟机动态迁移	—
		应允许云服务客户设置不同虚拟机之间的访问控制策略	(252)云计算安全	虚拟化防火墙、主机安全防护软件	通过部署虚拟化防火墙、主机安全防护软件，帮助云服务客户实现设置不同虚拟机之间的访问控制策略	基于虚拟化防火墙、主机安全防护软件，为云服务客户设置不同虚拟机之间的访问控制策略
	入侵防范	应能检测虚拟机之间的资源隔离失效，并进行告警	(252)云计算安全	虚拟化防火墙、主机安全防护软件	通过部署虚拟化防火墙、主机安全防护软件，检测虚拟机之间的资源隔离失效，并进行告警	基于虚拟化防火墙、主机安全防护软件，检测虚拟机之间的资源隔离失效，及时处置和汇报相关情况

表A.1　**云计算安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	入侵防范	应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警	(251)云计算管理	—	云平台本身的安全能力要求，应能检测非授权新建虚拟机或者重新启用虚拟机，进行告警	云平台本身的安全能力，应能检测非授权新建虚拟机或者重新启用虚拟机，进行告警，或者云平台接受第三方系统的监管实现相关能力
		应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警	(252)云计算安全	主机安全防护软件、安全资源池，虚拟化防火墙	基于病毒过滤等安全组件，检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警或阻断	基于病毒过滤安全组件，为虚拟机之间资源访问配置安全策略，实现恶意代码的检测和阻断
	镜像和快照保护	应针对重要业务系统提供加固的操作系统镜像	(251)云计算管理	主机安全防护软件	甲方应要求运维人员，针对重要业务系统采用加固的操作系统镜像进行安装部署	对重要业务系统，为甲方提供加固的操作系统镜像进行安装部署；及时打补丁；及时更新加固的镜像文件；私有云建设中，应将重要的应用进行区域划分，并在该区域中部署可统一进行虚拟机操作系统安全加固的管理软件，以确保操作系统内核、关键操作系统组件、端口、用户权限、进程等进行安全加固管
		应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改	(252)云计算安全	—	云平台本身应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改，如果云平台本身无校验功能，建议将镜像、快照文件导出进行手动的文件完整性校验	基于云平台本身应提供虚拟机镜像、快照完整性校验功能；如果云平台本身无校验功能，可以将镜像、快照文件导出进行手动的文件完整性校验

表A.1　云计算安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	镜像和快照保护	应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问	(210)文档安全管理	—	通过文档加密软件，将虚拟机镜像、快照中可能存在的敏感资源加密，防止被非法访问	为用户敏感资源提供加密手段，防止非法访问造成信息泄露;虚拟机镜像、快照在生成时采用加密或者设置租户访问权限等方式防止被其他角色访问；虚拟机多用来跑应用及业务系统，不能采用终端文档加密软件，否则影响用户访问
	数据完整性和保密性	应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定	—	—	甲方人员自己的云服务客户数据、用户个人信息等应存储于中国境内，如需出境应遵循国家相关规定	向甲方人员普及相关规定，确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定
		应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限	—	—	应对所有访问数据的行为日志进行审计，抽查是否有未授权的数据操作行为	根据日志审计系统的报警提示，加强对未授权数据操作行为的监管，及时提交审计分析报告
		应使用校验码或密码技术确保虚拟机迁移过程中，重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施	—	—	云服务商提供的虚拟化平台应具备保证重要数据完整性的能力，对虚拟化平台的该项能力进行测试验证	应制定详细的测试验证方案，定期进行测试

表A.1　**云计算安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	数据完整性和保密性	应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程	(225)虚拟专用网络设备	—	加强对客户使用的密钥管理系统的备案工作，同时尽可能进行整合，实现密钥管理系统的共享使用	配合甲方完成云平台上的数据加解密工作，保障数据安全性
	数据备份恢复	云服务客户应在本地保存其业务数据的备份	(236)本地数据备份	存储备份一体机，容灾备份一体机	通过备份设备在本地保存其业务数据的备份	定期进行本地保存业务数据的备份，定期检查备份数据的有效性，保障数据安全可用
		应提供查询云服务客户数据及备份存储位置的能力	(236)本地数据备份	—	云平台应提供查询云服务客户数据及备份存储位置的能力	协助甲方人员监督执行，云平台必须提供查询客户数据及备份存储位置的能力
		云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致	(238)异地数据备份、(239)异地数据恢复	存储备份一体机，容灾备份一体机	要求云服务商的云存储服务保证云服务客户数据存在若干可用副本，各副本内容保持一致	协助甲方人员监督执行，定期检查客户数据的多个副本，并通过演练测试各个数据副本之间数据内容的一致性
		应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程	(238)异地数据备份、(239)异地数据恢复	-	要求云服务商为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程	协助甲方人员监督执行，云计算服务提供商应具备将用户数据迁移出当前云计算平台的能力，有需要的话可以要求云服务提供商提供相关的安全演练，测试云服务提供商在相关场景下数据迁移的能力

表A.1 **云计算安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	剩余信息保护	应保证虚拟机所使用的内存和存储空间回收时得到完全清除	(251)云计算管理	—	云平台自身属性必须保证虚拟机所使用的内存和存储空间回收时得到完全清除	协助甲方人员监督执行，要求云服务提供商在必要时提供测试，检查虚拟机占用的内存和存储空间在回收时是否得到完全清除
		云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除	(251)云计算管理	—	云平台必须保证云服务客户删除业务应用数据时，云计算平台将云存储中所有副本删除	协助甲方人员监督执行，要求云服务提供商在必要时提供测试，检查云服务客户删除业务应用数据时，云平台将云存储中所有副本删除，所有业务操作在多方人员监督下执行并验证
安全管理中心	集中管控	应能对物理资源和虚拟资源按照策略做统一管理调度与分配	(251)云计算管理	-	云平台自身应能对物理资源和虚拟资源按照策略做统一管理调度与分配	云平台自身应能对物理资源和虚拟资源按照策略做统一管理调度与分配
		应保证云计算平台管理流量与云服务客户业务流量分离	(251)云计算管理	—	云平台自身应保证云计算平台管理流量与云服务客户业务流量分离	云平台自身应保证云计算平台管理流量与云服务客户业务流量分离
		应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计	(184)网络安全审	云安全资源池、虚拟化防火墙	云服务客户依据职责划分，基于安全资源池安全审计组件，收集自身控制部分的审计数据并实现集中审计功能	基于安全资源池安全审计组件，收集自身审计数据，进行审计工作，向甲方汇报审计工作

表A.1　**云计算安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全管理中心	集中管控	应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测	(251)云计算管理	—	云服务商应提供对自身和云服务客户的控制部分，如虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测	基于云平台提供的监测功能，实现包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测，定期向甲方汇报相关工作情况
安全建设管理	云服务商选择	应选择安全合规的云服务商，其所提供的云平台应为其所承载的业务应用系统提供相应等级的安全保护能力	(252)云计算安全	—	要求云服务商所提供的云平台为其所承载的业务应用系统提供相应等级的安全保护能力	做好云平台整体等级保护能力的审核
		应在服务水平协议中规定云服务的各项服务内容和具体技术指标	—	—	要求云服务商在服务水平协议中规定云服务的各项服务内容和具体技术指标	协助甲方做好云服务商服务水平协议的审核
		应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等	—	—	要求云服务商在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等	协助甲方做好云服务商服务水平协议的审核
		应在服务水平协议中规定服务合约到期时，完整地返还云服务客户信息，并承诺相关信息在云计算平台上清除	—	—	要求云服务商在服务水平协议中规定服务合约到期时，完整地返还云服务客户信息，并承诺相关信息在云计算平台上清除	协助甲方做好云服务商服务水平协议的审核

表A.1 **云计算安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全建设管理	云服务商选择	应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据	—	—	要求与选定的云服务商签署保密协议，云服务商不得泄露云服务客户数据和业务系统的相关重要信息	协助甲方做好云服务商保密协议的审核
	供应链管理	应确保供应商的选择符合国家有关规定	—	—	确保供应商的选择符合国家有关规定	按照相关规定要求，协助甲方人员对云计算供应商进行筛选
安全建设管理	供应链管理	应将供应链安全事件信息或威胁信息能够及时传达到云服务客户	—	—	要求供应链安全事件信息或威胁信息能够及时传达到云服务客户	密切关注云计算平台供应链安全事件或威胁信息，针对相关信息及时发现、及时处理，相关处理流程和处理结果及时反馈给甲方人员，重大决策问题在不影响事件处理时效性的前提下充分与甲方人员沟通配合
安全建设管理	供应链管理	应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取有关措施对风险进行控制	—	—	要求运维服务人员、云计算服务平台方将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取有关措施对风险进行控制	将云计算供应商的重要变更及时传达给甲方负责人，与甲方人员共同评估变更带来的安全风险，对现有业务系统可能带来的影响以及相关处置措施，做好事前预防工作
安全运维管理	云计算环境管理	云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定	—	—	将云计算平台的运维地点安置在中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定	运维服务人员对甲方云计算平台进行运维时的物理位置应在中国境内，如有特殊情况确实需要境外运维，应严格遵循相关国家规定进行安全运维。

附 录 B
（规范性附录）
移动互联安全

移动互联安全应符合表B.1的规定。

注：表B.1中的标准与规范要求是指国卫办规划发〔2018〕4号 全国医院信息化建设标准与规范（试行）中对网络与信息安全保障所提的要求。

表B.1 移动互联安全

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全物理环境	无线接入点的物理位置	应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰	（164）无线AP	无线AP、无线AP集中管理平台	在无线项目规划时就对无线覆盖情况进行考虑，避免过度覆盖和覆盖不足等情况	结合实地场地布局，对无线信号覆盖调优
安全区域边界	边界防护	应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备	—	—	网络结构设计层面，保障无线网络和有线网络之间的数据流通过无线接入网关	协助用户对网络结构进行设计
	访问控制	无线接入设备应开启接入认证功能，并支持采用认证服务器或国家密码管理机构批准的密码模块进行认证	（183）网络防火墙	防火墙	对无线网络和有线网络边界部署防火墙，访问控制策略精确到端口级，默认未放行的流量，拒绝数据包通过	对无线网络和有线网络边界部署防火墙，访问控制策略精确到端口级，默认未放行的流量，拒绝数据包通过
	入侵防范	应能够检测到非授权无线接入设备和非授权移动终端的接入行为	（194）入侵防范设备、（195）入侵检测设备、（198）网络安全入侵防范	无线入侵防御	采购无线入侵防御设备，对非法AP进行定位	采购无线入侵防御设备，对非法AP进行定位

表B.1 **移动互联安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全区域边界	入侵防范	应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为	(194)入侵防范设备、(195)入侵检测设备、(198)网络安全入侵防范	无线入侵防御	采购无线入侵防御设备，对非法AP进行定位	通过无线入侵防御设备,对非法AP进行定位
		应能够检测到无线接入设备的SSID 广播、WPS 等高风险功能的开启状态	(194)入侵防范设备、(195)入侵检测设备、(198)网络安全入侵防范	无线入侵防御	采购无线入侵防御设备，对针对无线接入设备的攻击行为进行检测和定位	通过无线入侵防御设备，对针对无线接入设备的攻击行为进行检测和定位
		应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等	(194)入侵防范设备、(195)入侵检测设备、(198)网络安全入侵防范	无线AP管理平台	通过无线AP管理平台，实时监测无线接入设备的SSID广播、WPS等高风险行为的开启状态	通过无线AP管理平台，定期向用户汇报无线设备的SSID广播、WPS等高危功能的开启情况
		应禁止多个AP使用同一个认证密钥	(163)无线控制器AC	无线认证	避免多AP使用同一密钥认证的行为	—
		应能够阻断非授权无线接入设备或非授权移动终端	(196)网络准入控制设备	无线网络准入、IP地址管理	使用网络准入系统，对入网的有线、无线设备做一体化网络准入认证功能	—
安全计算环境	移动终端管控	应保证移动终端安装、注册并运行终端管理客户端软件	(221)移动终端安全管理	移动设备管理系统、虚拟化移动设备	移动终端管理客户端应具有防卸载功能，如确实需要卸载，必须有完善的审批流程	配合甲方人员做好终端管理客户端防卸载工作，确实需要卸载的，配合用户做审批流程，审批通过后可完成卸载

表B.1 **移动互联安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	移动终端管控	移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等	(220)桌面终端安全管理、(221)移动终端安全管理	终端安全管理系统、移动设备管理系统、虚拟化移动设备	采购的移动终端管理设备应具有设备生命周期管理、设备远程控制、设备安全管控等功能	做好移动终端设备全生命周期管理、设备安全管控等工作，并定期向甲方人员汇报工作情况
	移动应用管控	应具有选择应用软件安装、运行的功能	(221)移动终端安全管理	移动设备管理系统、虚拟化移动设备	采购的移动终端管理设备应具有具有选择应用软件安装、运行的功能，如禁止安装聊天软件，禁止安装网络视频软件的能力	协助甲方人员对移动终端管理设备的功能测试，设备必须具备自主选择相关应用软件进行安装和运行的功能，否则项目采购时对此供应商的提供的产品不予考虑
		应只允许指定证书签名的应用软件安装和运行	(221)移动终端安全管理	移动设备管理系统、虚拟化移动设备	采购的移动终端管理设备应具有具有对安装的软件进行证书签名验证的功能，确保只允许指定证书签名的应用软件安装和运行	协助甲方人员对移动终端管理设备的功能测试，测试设备必须具有对安装的软件进行证书签名验证的功能，确保只允许指定证书签名的应用软件安装和运行的功能，否则项目采购时对此供应商的提供的产品不予考虑
	移动应用管控	应具有软件白名单功能，应能根据白名单控制应用软件安装、运行	(221)移动终端安全管理	移动设备管理系统、虚拟化移动设备	通过终端本身的软件白名单功能或者移动终端安全管理设备的应用市场模块，指定可安装的应用，对相关应用做白名单放行	做好软件应用的的管控工作，禁止非授权软件应用系统的使用，定期向甲方人员汇报相关情况

表B.1 **移动互联安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全建设管理	移动应用软件采购	应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名	(221)移动终端安全管理	移动设备管理系统、虚拟化移动设备	通过移动终端管理设备对移动应用软件的分发渠道和证书签名进行核实，保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名	协助甲方人员监督执行，设备采购前邀请多家设备供应商进行功能测试，测试的移动设备管理系统必须具备对移动应用软件的分发渠道和证书签名进行验证的功能
		应保证移动终端安装、运行的应用软件由指定的开发者开发	—	—	甲方管理人员对移动应用软件的开发者进行监督，如移动应用软件开发商在项目中标后必须接受监督，软件开发人员必须是项目中标商的开发人员，非第三方外包公司人员进行开发，保障开发人员的能力符合资质要求，确保后期应用软件的稳定可靠和安全性	协助甲方人员进行监督，防止移动应用软件开发商将开发工作进行转包给不具备相应开发能力的人员或者组织，必须由中标商自行开发完成
	移动应用软件开发	应对移动业务应用软件开发者进行资格审查	—	—	在软件开发招投标阶段对移动业务应用软件开发者进行严格的资格审查，不满足资格要求的一律不予考虑	协助甲方人员进行监督，对移动业务应用软件开发者进行严格的资格审查，不满足资格要求的一律不予考虑

表B.1 **移动互联安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全建设管理	移动应用软件开发	应保证开发移动业务应用软件的签名证书合法性	(221)移动终端安全管理	移动设备管理系统、虚拟化移动设备	采购测试的移动设备管理系统必须具备对移动业务应用软件签名证书合法性进行鉴别的功能	协助甲方人员进行项目采购前的设备测试，测试的移动设备管理系统应具备对移动业务应用软件签名证书合法性进行校验的功能，否则在采购时对设备供应商提供的设备不予考虑
安全运维管理	配置管理	应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别	(221)移动终端安全管理	移动设备管理系统	对无线接入设备和移动终端进行识别，对非法无线接入设备和非法移动终端接入相关网络进行处置，如隔离审批或拒绝入网等	协助甲方人员进行项目采购前的设备测试，测试的移动设备管理系统应具备对对无线接入设备和移动终端进行识别，对非法无线接入设备和非法移动终端接入相关网络进行处置，如隔离审批或拒绝入网等，否则相关供应商提供的产品在项目采购时不予考虑

附 录 C
（规范性附录）
物联网安全

物联网安全应符合表C.1的规定。

注：表D.1中的标准与规范要求是指国卫办规划发〔2018〕4号 全国医院信息化建设标准与规范（试行）中对网络与信息安全保障所提的要求。

表C.1 物联网安全

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全物理环境	感知节点设备物理防护	感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动	—	—	甲方人员应对感知节点设备附近物理安全防护，防破坏措施进行考量	运维服务人员在感知节点设备布放时应考虑到环境可能对其造成的物理损害，并尽量避免
		感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）	—	—	针对环境、RFID、红外、视频接入等节点的特性要求配置感知节点部署条件，确保感知节点能正确反应环境状态	运维服务人员应确保感知节点设备布放在合适位置，设备工作时所处的物理环境能够正常反映环境状态
		感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等	—	—	根据感知节点设备工作环境要求，避免设备的正常工作被干扰	运维服务人员在感知节点布放时进行监督，避免感知节点设备所处的物理环境干扰设备的正常运行
		关键感知节点设备应具有可供长时间工作的电力供应（关键网关节点设备应具有持久的，稳定的电力供应能力）	—	充电桩、备用电源(UPS等),采用软件系统对感知节点设备供电状况进行监测	甲方在项目采购时应选择质量稳定可靠的电力供应设备，元器件等	运维服务人员应定期检查感知节点设备的电力供应情况，防止供电不足或断电

表C.1 **物联网安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全区域边界	接入控制	应保证只有授权的感知节点可以接入	二十二、物联网技术(七十八）物联网应用	防火墙、安全路由器、网络准入设备、IP地址管理、4A	采购网络准入设备，对被授权的感知节点进行资产录入，未授权的感知节点拒绝入网或者进行入网审核	协助甲方人员，将节点纳入物联网网络认证中心，拒绝未纳入的感知节点入网
	入侵防范	应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为	二十二、物联网技术(七十八）物联网应用	防火墙、安全路由器、访问控制设备，采用入侵检测、入侵防御设	定期查看运维服务人员提供的感知节点对外的攻击行为报告，进行安全处置	运维服务人员应采用攻击检测、攻击防御设备对网络攻击行为进行实时检测和阻断，对由网络内部向外攻击的设备，进行网络隔离处置；对于外部攻击行为，将相应攻击IP加入黑名单，拒绝其网络访问请求
		应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为	二十二、物联网技术(七十八）物联网应用	防火墙、安全路由器、访问控制设备	采购具有入侵检测、入侵防御功能的网关节点	定期分析入侵检测、入侵防御行为报告，向甲方人员汇报相关网络攻击情况和处置建议
安全计算环境	感知节点设备安全	应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更	二十二、物联网技术(七十八）物联网应用	采用物联网安全平台或设备自带的管理系统管理	用网管软件管理感知节点设备，对节点管理账号进行明确的权限划分	定期审计感知节点管理账户的操作行为
		应具有对其连接的网关节点设备(包括读卡器）进行身份标识和鉴别的能力	二十二、物联网技术(七十八）物联网应用	物联网安全网关	与国家物联网标识管理公共服务平台（南沙分中心）对接，将感知节点设备进行统一标识管控	定期检查感知结点设备与国家物联网标识管理公共服务平台(南沙分中心）的对接情况

表C.1 **物联网安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	感知节点设备安全	应具有对其连接的其他感知节点设备(包括路由节点)进行身份标识和鉴别的能力	二十二、物联网技术(七十八）物联网应用	—	感知节点自身应具备对其连接的其他感知节点设备(包括路由节点）进行身份标识和鉴别的能力	—
	网关节点设备安全	应具备对合法连接设备(包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力	(196)网络准入控制设备	安全路由器，网管软件	网关节点应具备对合法连接设备(包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力	将节点纳入物联网网络认证中心
	网关节点设备安全	应具备过滤非法节点和伪造节点所发送的数据的能力	(183)网络防火墙	安全路由器	网关节点应具备过滤非法节点和伪造节点所发送的数据的能力	将节点纳入物联网网络认证中心
		授权用户应能够在设备使用过程中对关键密钥进行在线更新	(226)加密机设备	安全路由器	授权用户应具备在网关节点设备使用过程中对关键密钥进行在线更新的能力	定期检查监督执行
		授权用户应能够在设备使用过程中对关键配置参数进行在线更新	(226)加密机设备	安全路由器	授权用户应能够在网关节点设备使用过程中对关键配置参数进行在线更新的能力	定期检查监督执行
	抗数据重放	应能够鉴别数据的新鲜性，避免历史数据的重放攻击	(226)加密机设备	加密机、VPN	采购加密机，对数据通道进行 IPSEC 协议加密	采用加密机进行加密通道数据传输
		应能够鉴别历史数据的非法修改，避免数据的修改重放攻击	(226)加密机设备	加密机、VPN	采购加密机，对数据通道进行 IPSEC 协议加密	采用加密机进行加密通道数据传输

表C.1 **物联网安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全运维管理	感知节点管理	应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护	(262)资产和物资管理	—	督促运维服务提供商对感知节点进行巡检和维护，并对相关情况进行记录和上报	运维服务人员定期对感知节点进行巡检和维护，并对相关情况进行记录和上报甲方
		应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理	(262)资产和物资管理	—	甲方管理人员要求运维服务提供商加强感知节点全生命周期流程管理	运维服务人员应对感知节点资产进行全生命周期管理，定期上报相关资产变更行为
		应加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等	(262)资产和物资管理	—	甲方人员应具备保密意识，加强对感知节点设备的部署环境保密性管理和对相关负责人的管理	运维服务人员应按照相关保密级别要求，对感知节点部署环境进行保密；如有调岗，应立即交还相关检查工具和维护记录等

附 录 D
（规范性附录）
工控系统安全

工控系统安全应符合表D.1的规定。

注：表D.1中的标准与规范要求是指国卫办规划发〔2018〕4号 全国医院信息化建设标准与规范（试行）中对网络与信息安全保障所提的要求。

表D.1 工控系统安全

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全物理环境	室外控制设备物理防护	室外控制设备应放置于采用铁板或其他防火绝缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；控制设备应安装在金属或其它绝缘板上(非木质板)，并紧固于箱体或装置中	—	—	要求控制设备外围箱体采用加固式三防材料制作	定期检查，监督执行、做好巡检记录
		室外控制设备放置应远离强电磁干扰、强热源等的环境，如无法避免应及时做好应急处置及检修保证设备正常运行	—	—	设定电磁强度和温度的可接受范围，制定相应的应急措施；可使用电磁屏蔽柜、绝热材料等进行隔离	定期评估电磁强度和温度等环境因素是否发生明显变化；做好巡检记录

表D.1 **工控系统安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全通信网络	网络架构	工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用单向的技术隔离手	—	单向网闸	要求使用单向网闸，控制数据流向，制定相关控制策略；工业控制系统与企业其他系统之间存在安全区高低之分，高低安全区之间数据传输时应使用单方向传输的隔离设备；也可通过Vlan划分方式进行区域业务划分	不同区域之间是否存在绕过隔离装置进行数据交互、隔离装置策略是否严谨合规;优化策略、做好巡检记录
		工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段	—	工业防火墙	要求根据业务重要性等划分不同安全域，在不同安全域之间设置访问控制规则，关闭不必要的端口	检查不同安全域是否启用了访问控制策略；核查策略的合理性，精细度，并优化配置；出相应报告
		涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网，在物理层面上实现与其它数据网及外部公共信息网的安全隔离	—	工业防火墙、单向网闸	要求实时控制系统单独组网，与其他数据网强隔离	检查是否启用了强隔离措施；核查策略的合理性、精细度并优化配置；出相应报告
	通信传输	在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输	—	—	要求启用IPSEC、MD5.SSL、SSH等加密技术	检查是否在通信过程中采取保密措施；验证在通信过程中是否对数据进行加密；出具检查报告和加固建议

表D.1 **工控系统安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全区域边界	访问控制	工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的E-Mail、Web、Telnet、Rlogin、FTP等通用网络服务	—	工业防火墙	要求工业控制系统与企业其他系统之间部署工业防火墙，制定基本的防火墙策略(明确指定端口进行跨越边界的网络通信，指定端口配置并启用了安全策略；工业控制系统与企业其他系统之间应部署访问控制设备，且访问控制策略支持通用IT网络服务，包括e-mail、Web、Telnet、Rlogin、FTP等；在访问控制策略中，禁用上述通用网络服务，在保证业务通讯正常条件下，以最小化为原则，禁用一切其他策略	采用技术手段核查或测试验证是否存在其他未受控端口跨越边界；定期分析防火墙日志；根据业务需求优化防火墙策略；出相应报告
		应在工业控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警	—	工业防火墙、工控审计平台	要求在安全域之间实时监测边界防护机制有效性，制定相关应急措施；应急措施包括手工配置区域之间的访问策略，例如通过网络设备自带的acl进行管控	采用技术手段测试验证失效报警功能；定期分析防火墙、审计系统日志；提出改进措施并出相应报告

表D.1 工控系统安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全区域边界	访问控制	应在工业控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警	—	工业防火墙、工控审计平台	要求在安全域之间实时监测边界防护机制有效性，制定相关应急措施；应急措施包括手工配置区域之间的访问策略，例如通过网络设备自带的acl进行管控	采用技术手段测试验证失效报警功能;定期分析防火墙、审计系统日志;提出改进措施并出相应报告
	拨号使用控制	工业控制系统确需使用拨号访问服务的，应限制具有拨号访问权限的用户数量；并采取用户身份鉴别和访问控制等措施	—	工业防火墙、工控主机安全防护系统	要求设定拨号数量，制定拨号相关的身份及权限范围	测试拨号的合规合法性;定期分析防火墙、主机防护系统的日志;提出改进措施并出相应报告
		拨号服务器和客户端均应使用经安全加固的操作系统，并采取数字证书认证、传输加密和访问控制等措施	—	CA、主机加固软件、防病毒软件	要求采用安全操作系统，要求启用IPSEC、SSH等	定期对系统进行加固；检查ipsec、SSH等有效性,定期更改相关密码;出相应报告
	无线使用控制	应对所有参与无线通信的用户(人员、软件进程或者设备）提供唯一性标识和鉴别	—	CA、无线安全网关、无线安全AP，移动应用管理系统(MAM)、CA Key、手机动态认证码、指纹识别	在借助于运营商（无线）网络的组网中，需要对通信端（通信应用设备或通信网络设备）建立基于用户的标识（用户名、证书等),标识具有唯一性且支持对该属性进行鉴别；在工业现场自建无线（WiFi、zigbee等）网络中，通信网络设备应在组网过程中具备唯一标识，且支持对该设备属性进行鉴别，并且使用强身份认证措施	定期检查无线使用的情况，覆盖面、身份鉴别措施是否符合要求,提出优化建议

表D.1 工控系统安全（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全区域边界	无线使用控制	应对所有参与无线通信的用户(人员、软件进程或者设备）进行授权以及执行使用进行限制	—	无线安全网关、无线安全AP，移动引用管理系统（MAN）	要求对于不同用户分配不同的账号和权限进行规定。无线通信中的应用设备或网络设备需支持对无线通讯策略进行授权，非授权设备或应用不能接入无线网络；非授权功能不能在无线通信网络中执行响应动作，对于授权用户需要具备权限控制策略	定期检查账号、密码、权限分割等情况,提出优化建议，出具报告
		应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护	—	无线安全网关、无线安全AP、SSL、MD5	要求采用SSL、MD5等加密协议，规定加密强度策略；要求定期对相关行为日志进行审计分析	定期检查，定期对日志进行审计分析，出具报告
		对采用无线通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统行为	—	无线安全网关、无线安全AP，移动应用管理系统(MAM)	制定未授权无线设备的处理措施；在应用无线通信技术的工业生产环境，应具备识别、检测工业环境中其他未授权无线设备射频信号的应用，并对未授权的无线接入行为及应用进行审计、报警及联动管控，避免无线信号干扰影响生产、避免未授权用户通过无线接入控制系统对生产造成破坏	定期测试无线信号射频范围，排查非授权无线设备，出具检查报告

表D.1 **工控系统安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	控制设备安全	控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等设备和计算方面的安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制	—	CA、工业防火墙、工控审计平台	提出相应的安全要求，制定替代措施；考虑到控制系统自主可控范围较低，在其自身不满足上述条件时，需通过上位控制系统或其他管理设备实现上述要求	定期检查，定期分析相关安全设备的日志，提出优化建议
		应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作	—	补丁管理软件	要求更新前进行回滚测试；工业生产环境的特殊性（应用兼容性较弱），在对控制设备进行补丁更新、固件更新时，需要对控制系统进行充分的验证、兼容性测试、评估后，在停产维修阶段对系统进行更新升级，保障控制系统的可用性	定期做好备份工作，在升级时具备还原能力；定期检查是否最新，实行加固服务，出具报告
		应关闭或拆除控制设备的软盘驱动、光盘驱动、USB接口、串行口或多余网口等，确需保留的必须通过相关的技术措施实施严格的监控管理	—	工控安全检查工具箱	为避免通过不必要的外设接口对工业系统造成破坏，需将控制设备的软驱、光驱、USB接口、串口及多余网口进行拆除或屏蔽，如不具备拆除条件或需保留的，应通过管理措施进行严格管控	定期检查、安全加固、提出优化建议

表D.1 **工控系统安全**（续）

层面	控制点	等保2.0要求	标准与规范要求	软硬件系统	管理视角	运维服务视角
安全计算环境	控制设备安全	应使用专用设备和专用软件对控制设备进行更新	—	工控漏扫、工控等保工具箱	规定使用专用设备和专用软件的范围；控制设备更新需采用专用硬件，确保运维版本控制，控制系统更新均为专用软件	定期检查，监督执行
		应保证控制设备在上线前经过安全性检测，保证控制设备固件中不存在恶意代码程序	—	工控安全检查工具箱、杀毒U盘	要求控制设备经过严格的安全合规性测试；使用经过权威机构认证的检测工具针对工控设备进行安全检测，在满足合规条件下允许并网投运	病毒查杀、安全基线核查、提出优化建议
安全建设管理	产品采购和使用	工业控制系统重要设备及专用信息安全产品应通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测后方可采购使用	—	—	要求经过相关权威机构的认证，说明认可的证书范围	定期检查，监督执行
	外包软件开发	应在外包开发合同中包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款	—	—	应该与外包公司及控制设备提供商签署保密协议或合同，以保证其不会将本项目重要建设过程及内容进行宣传及案例复用，目的在于保障工业企业在建设时期的敏感信息、重要信息等内容不被泄露	根据实际情况提出保密协议的修改建议

附 录 E
（规范性附录）
网络与信息安全软硬件系统（产品）基本功能和性能指标

E.1 概述

本附录给出了与网络和信息安全密切相关的43个主流产品的多项基本功能和性能指标。列出的这些软硬件系统都是市面上通行的安全产品，而所列的功能和性能指标也不出现特定厂商的特定参数。

E.2 网络防火墙

E.2.1 基本要求

应拥有自主知识产权。

E.2.2 操作系统

建议采用冗余设计。

E.2.3 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.2.4 工作模式

支持路由、交换、混合、虚拟线工作模式。

E.2.5 主要功能

E.2.5.1 路由交换

支持静态路由、动态路由、策略路由。

E.2.5.2 高可用

支持链路聚合、端口联动、双机热备。

E.2.5.3 IPv6支持

支持IPv4/IPv6双栈工作模式。

E.2.5.4 地址转换

支持IPv4/ IPv6网络环境下的地址转换。

E.2.5.5 身份认证

支持本地认证和第三方外部认证方式。

E.2.5.6 用户管控

利用身份认证与访问控制技术实现安全防护策略

E.2.5.7 访问控制

支持基于五元组信息、用户、域名、应用、服务、时间、安全引擎等的访问控制。

E.2.5.8 连接控制

支持对单条访问控制策略进行最大并发连接数限制。

E.2.5.9 系统诊断

提供诊断系统网络连通性的工具。

E.2.5.10 安全审计

提供完善的审计数据查询功能，方便管理员进行审查和分析，支持独立配置审计策略，同时也可将指定的 IP 地址、 URL、 应用加入白名单，不进行数据审计。

E.2.5.11 流量统计

应支持根据应用对通过设备的数据报文流量进行统计，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、新建连接数、当前会话数以及流速。

E.2.5.12 威胁统计

应支持按照威胁类型/攻击者/受害者等方式进行威胁排名。

E.2.5.13 网络日志

支持日志本地存储，可对不同类型日志设置存储空间；支持外发至SYSLOG服务器，可将多条日志合并成一条日志传送到日志服务器中，可选择对日志传输是否加密。

E.2.5.14 数据报表

内置预定义报表模板，支持根据通信流量、上网行为、威胁统计等来源数据库自定义报表模板；支持报表导出。

E.2.5.15 资源监控

可对CPU/内存/磁盘占用率等设置阈值。

E.2.6 性能要求

E.2.6.1 防火墙吞吐率

应与实际网络带宽相匹配并对未来业务量增长有足够冗余。

E.2.6.2 应用层吞吐率

应与实际HTTP/HTPPS/SMTP/IMAP等应用所需网络带宽相匹配，并有业务增长冗余考虑。

E.2.6.3 最大并发连接数

应满足实际网络环境中用户访问各种应用产生的会话连接数之和并有冗余考虑。

E.2.6.4 每秒新建连接数

应满足每秒通过防火墙建立完整的TCP/UDP连接数的要求。

E.2.7 其他安全模块

支持扩展GRE/IPSEC/SSL VPN接入、应用识别、病毒防护、入侵防御等功能。

E.3 分布式防火墙

E.3.1 基本要求

应拥有自主知识产权。

E.3.2 平台兼容性

应使用虚拟化平台原厂预留的安全接口组件进行防护，不可使用官方停止维护的接口组件进行防护。

E.3.3 性能要求

E.3.3.1 并发连接数

应满足实际网络环境中用户访问各种应用产生的会话连接数之和并有冗余考虑。

E.3.3.2 防火墙吞吐率

应与实际网络带宽相匹配并对未来业务量增长有足够冗余。

E.3.4 主要功能

E.3.4.1 集中管理

应支持集中管理、策略下发、事件收集、日志审计、报表统计等。

E.3.4.2 虚拟机感知

应支持从虚拟化平台获取虚拟机信息，包括虚拟机名字，IP地址等，应用于安全策略配置。

E.3.4.3 防护范围

支持防护物理网络进出虚拟机和同一物理服务器上虚拟机之间的网络流量。

E.3.4.4 策略迁移

应支持虚拟机的迁移、复制情况下，同步调整安全策略。

E.3.4.5 流量可视化

应支持虚拟机通信量（源地址，目的地址，源端口，目的端口）排名。

E.3.4.6 面向对象的安全策略

应支持以操作系统、虚机名称、安全标签、安全组等多种业务属性来编写安全策略。

E.3.4.7 Bypass功能

当虚拟化安全网关出现异常时，在Hypervisor层bypass虚拟机流量，保障业务通信。

E.3.5 模块化设计

应支持扩展防病毒、入侵防御、安全审计等功能。

E.4 工控防火墙

E.4.1 基本要求

应拥有自主知识产权。

E.4.2 部署方式

应支持路由、透明、混合模式接入。

E.4.3 物理接口要求

千兆电口，千兆光口等按需选择。

E.4.4 产品性能

E.4.4.1 并发连接数

应满足实际网络环境中各种会话连接数之和、且有冗余考虑。

E.4.4.2 防火墙吞吐率

应与实际网络带宽相匹配并对未来业务量增长有足够冗余。

E.4.5 主要功能

E.4.5.1 账户管理

应支持基于角色的账户管理，支持管理员三权分立。

E.4.5.2 诊断文件下载

应支持系统错误诊断文件下载，方便进行问题定位。

E.4.5.3 接口参数

应支持网络接口MTU、链路模式自定义，满足不同组网要求。

E.4.5.4 工业协议

应支持Modbus TCP、OPC、IEC 60870-5-104、S7等协议解析，支持定制开发自定义协议。

E.4.5.5 深度防护

应支持对工业协议的完整性、功能码、地址范围与读写权限、工艺参数值范围等深度解析与过滤控制。

E.4.5.6 工控指令控制

应根据控制器所使用协议的不同，灵活进行线圈、寄存器读写权限控制、读写地址控制。

E.4.5.7 OPC动态防护

应支持自动检测协议状态，无需端口全开，动态控制端口开放。

E.4.5.8 攻击防护

应支持DOS攻击防护、ARP攻击防护等。

E.4.5.9 会话管理

应支持基于源或者目标限制每个IP的最大连接和超时时间。

E.4.5.10 VPN

应支持IPSEC VPN功能。

E.5 Web防火墙

E.5.1 部署方式

应支持透明串联、旁路监测、负载均衡、反向代理等部署方式。

E.5.2 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.5.3 性能要求

E.5.3.1 并发连接数

满足实际网络环境中各种Web访问会话连接数之和、且有冗余考虑。

E.5.3.2 防火墙吞吐率

应与实际Web业务带宽相匹配并对未来业务量增长有足够冗余。

E.5.4 基本功能

E.5.4.1 链路聚合

应支持链路聚合功能，提高链路带宽。

E.5.4.2 路由支持

应支持静态路由和策略路由。

E.5.4.3 服务器检查

应支持服务器健康检查，实时监测服务器的活跃状态。

E.5.4.4 IPv6兼容性

应支持在IPv6环境下部署和运行。

E.5.4.5 协议合规

应支持对用户请求数据做合规性检查。

E.5.4.6 WEB安全规则库

应提供专业的WEB安全规则库并定期更新。

E.5.4.7 WEB防护

应支持阻断SQL注入攻击、跨站脚本(XSS)攻击、web shell后门上传防护、爬虫防护、盗链防护、暴力登录防护等。

E.5.4.8 文件控制

应支持对文件上传、下载做控制。

E.5.4.9 WEB漏洞扫描

应支持WEB应用漏洞的安全扫描检测。

E.5.4.10 负载均衡

应支持多服务器的负载均衡，提供多种负载均衡算法。

E.5.4.11 日志管理

日志应支持多条件查询和外发给第三方日志平台。

E.5.4.12 系统管理

应支持多种故障诊断方式，支持配置文件导入、导出，支持规则库的在线和离线升级，支持各种告警通知方式。

E.5.4.13 双机热备

应支持双机热备。

E.5.4.14 硬件Bypass

应支持断电bypass模式。

E.6 数据库防火墙

E.6.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.6.2 性能要求

E.6.2.1 DB最大并发数

应满足实际网络环境中DB访问会话连接数之和、且有冗余考虑。

E.6.2.2 SQL处理能力

应与实际DB业务带宽相匹配并对未来业务量增长有足够冗余。

E.6.3 基本功能

E.6.3.1 部署方式

应支持旁路和串联部署。

E.6.3.2 数据库兼容性

应支持Oracle、MSSQL、DB2、Sybase、Informix、MYSQL、金仓、神通、达梦等主流数据库。

E.6.3.3 审计功能

审计记录应包括时间、用户名、操作终端主机名及IP地址等信息。

E.6.3.4 审计规则设置

应支持各种组合审计规则。

E.6.3.5 访问控制

应支持对超过指定行数的修改、删除、查询和添加行为进行限制。

E.6.3.6 数据库防护

应支持主动监控数据库活动，防止未授权的数据库访问、权限或角色升级，以及对敏感数据的非法访问等。

E.6.3.7 白名单控制

应支持黑白名单的访问控制，以IP地址、用户、应用程序、时间段等为授权单位，进行访问控制。

E.6.3.8 暴力破解防护

应能够对过于频繁访问数据库的IP地址进行访问控制限定，防止非法访问数据库或口令暴力破解。

E.6.3.9 访问自学习

应支持自学习功能，能够基于自学习机制主动监控数据库活动，防止未授权的非法数据库访问。

E.6.3.10 服务发现

应支持根据常用端口号、自定义端口号发现指定网段范围内存在的数据库服务。

E.6.3.11 敏感数据发现

应支持对指定的数据库进行敏感数据扫描，发现数据库中敏感数据的分布情况。

E.6.3.12 风险扫描

应支持扫描发现数据库中存在的安全风险、弱口令等。

E.6.3.13 虚拟补丁

应支持对已公开的数据库漏洞攻击行为拦截。

E.6.3.14 审计分析

应支持关键字分析与统计分析等，对各种应用的流量、访问行为进行统计。

E.6.3.15 日志管理

支持按日志属性、日志类型、时间范围进行分类，同时支持日志外发功能。

E.6.3.16 数据库监控

应支持通过监控数据库系统的各种信息来判断数据库系统是否正常，保证数据库的可用性。

E.6.3.17 报表功能

应内置各种报表，同时支持自定义报表功能。

E.6.3.18 账户管理

应支持管理员权限分权管理，提供三权分立功能。

E.7 。病毒过滤网关

E.7.1 基本要求

应为专业的防病毒网关，非UTM、防火墙等的防病毒模块。

E.7.2 操作系统

应具有双系统，且支持多核环境。

E.7.3 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.7.4 性能要求

E.7.4.1 最大并发连接数

应满足实际网络环境中访问会话连接数之和、且有冗余考虑。

E.7.4.2 病毒检测吞吐率

应与实际业务带宽相匹配并对未来业务量增长有足够冗余。

E.7.5 工作模式

支持路由、交换、混合、虚拟线工作模式。

E.7.6 主要功能

E.7.6.1 病毒过滤

建议采用双库技术，避免单一病毒库的漏查，漏杀。

E.7.6.2 病毒病毒检测能力

应能够防御病毒、木马、蠕虫、间谍软件等恶意软件，支持对压缩数据、加壳病毒的检测与处理。

E.7.6.3 协议支持

应支持对HTTP、FTP、POP3、 SMTP、IMAP等常用协议进行病毒检测与过滤。

E.7.6.4 蠕虫防护

可实时检测蠕虫攻击，并进行阻断。

E.7.6.5 多层压缩文件查杀

应具备多层的数据解压缩病毒查杀能力。

E.7.6.6 双栈支持

支持IPv4和IPv6双栈协议的病毒扫描与检测过滤。

E.7.6.7 检测率要求

对流行病毒检测率不低于95%，建议提供相关机构的病毒检测率报告。

E.7.6.8 病毒库

应具有独立的蠕虫防护规则库，支持手动或自动方式升级。

E.7.6.9 手机病毒检测

应具有手机病毒特征库。

E.7.6.10 URL过滤

应支持URL过滤方式阻止非法数据进入内部网络。

E.7.6.11 邮件过滤

应具有邮件主题关键字过滤、附件名称过滤、带密码保护的附件过滤等。

E.7.6.12 文件传输控制

应支持自定义禁止传输的文件类型。

E.7.6.13 黑白名单支持

应支持基于IP地址黑白名单、邮件地址黑白名单的垃圾邮件过滤。

E.7.6.14 多接口监听

应支持多接口可旁路的病毒监听检测模式，可并行监听检测多条链路内的病毒传输行为。

E.7.6.15 多通道防护

应支持利用同一台病毒过滤网关实现多链路多区域的病毒防护。

E.7.6.16 日志记录

应提供完整的病毒日志、访问日志和系统日志等，并可根据日志数据生成报表。

E.7.6.17 系统监控

应支持监控系统资源、网络流量、当前会话数、当前病毒扫描信息等。

E.7.6.18 病毒隔离与取证

应支持病毒隔离功能，管理员可选择把隔离区的内容删除，或将隔离内容发送到多个邮箱进行后期的分析取证。

E.7.6.19 病毒警告

应支持邮件报警、声音报警、SNMP等报警方式。

E.7.6.20 日志外发

应支持多个Syslog远程日志服务器，可将不同类型的日志发送到不同服务器进行分析。

E.8 入侵防御

E.8.1 基本要求

应拥有自主知识产权。

E.8.2 操作系统

建议采用冗余设计。

E.8.3 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.8.4 工作模式

建议支持直连、路由、旁路监听、混合部署等多种模式。

E.8.5 性能要求

E.8.5.1 整机吞吐率

应与实际网络业务带宽相匹配并对未来业务量增长有足够冗余。

E.8.5.2 IPS吞吐率

应满足实际网络环境中各种攻击流量会话连接数之和并有冗余考虑。

E.8.6 主要功能

E.8.6.1 路由交换

应支持静态路由、动态路由、策略路由。

E.8.6.2 高可用

应支持链路聚合、端口联动、双机热备。

E.8.6.3 IPv6支持

应支持IPv4/IPv6双栈工作模式。

E.8.6.4 规则库

攻击规则库、应用识别库、URL过滤库、病毒库单独分开，应支持手动、自动、以及离线升级。

E.8.6.5 流量采集

应支持对服务器地址、端口、以及采样百分比进行设置。

E.8.6.6 规则自定义

应支持自定义攻击检测规则。

E.8.6.7 黑名单

应支持将攻击源加入黑名单，一段时间内禁止访问。

E.8.6.8 攻击取证

检测到攻击事件后，应将报文记录下来，作为电子证据。

E.8.6.9 流量异常检测

应支持对设备接口流量阀值进行设置及报警。

E.8.6.10 DDOS防御

应支持独立的DDOS检测、阻断及基线自学习的能力。

E.8.6.11 连接数限制

应支持主机并发连接数、半连接数限制。

E.8.6.12 应用识别

系统应根据数据内容而非端口智能识别各类应用。

E.8.6.13 应用管理

应支持灵活的应用管理策略，实现多维度的监控。

E.8.6.14 无线攻击防御

应能检测阻断钓鱼攻击。

E.8.6.15 无线安全区

应支持对WIFI进行屏蔽、检测无线AP风险配置。

E.8.6.16 无线定位

应支持定位非法AP。

E.8.6.17 日志存储

应支持多种形式的日志存储,如本地存储、外发等方式。

E.8.6.18 告警方式

系统应提供邮件、声音、SNMP多形式的告警方式。

E.8.6.19 登录防护

支持登陆界面图形验证码，防止管理员账号被暴力破解。

E.8.7 其他安全模块

含攻击规则库特征库 ，可扩展WEBFILTER功能规则库、病毒过滤规则库、无线入侵防御功能。

E.9 入侵检测

E.9.1 基本要求

应拥有自主知识产权

E.9.2 操作系统

建议采用冗余设计。

E.9.3 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.9.4 性能要求

E.9.4.1 整机吞吐率

应与实际网络业务带宽相匹配并对未来业务量增长有足够冗余。

E.9.4.2 IDS吞吐率

应满足实际网络环境中需要进行镜像分析的各种攻击流量会话连接数之和并有冗余考虑。

E.9.5 主要功能

E.9.5.1 路由交换

应支持静态路由、动态路由、策略路由。

E.9.5.2 高可用

应支持链路聚合、端口联动、双机热备。

E.9.5.3 IPv6支持

应支持IPv4/IPv6双栈工作模式。

E.9.5.4 规则库

攻击规则库、应用识别库、URL过滤库、病毒库单独分开，应支持手动、自动、以及离线升级。

E.9.5.5 流量采集

应支持对服务器地址、端口、以及采样百分比进行设置。

E.9.5.6 规则自定义

应支持自定义攻击检测规则。

E.9.5.7 黑名单

应支持将攻击源加入黑名单，一段时间内禁止访问。

E.9.5.8 攻击取证

检测到攻击事件后，应将报文记录下来，作为电子证据。

E.9.5.9 流量异常检测

应支持对设备接口流量阀值进行设置及报警。

E.9.5.10 DDOS防御

应支持独立的DDOS检测、阻断及基线自学习的能力。

E.9.5.11 连接数限制

应支持主机并发连接数、半连接数限制。

E.9.5.12 应用识别

系统应根据数据内容而非端口智能识别各类应用。

E.9.5.13 应用管理

应支持灵活的应用管理策略，实现多维度的监控。

E.9.5.14 无线攻击防御

应能检测阻断钓鱼攻击。

E.9.5.15 无线安全区

应支持对WIFI进行屏蔽、检测无线AP风险配置。

E.9.5.16 无线定位

应支持定位非法AP。

E.9.5.17 日志存储

应支持多种形式的日志存储,如本地存储、外发等方式。

E.9.5.18 告警方式

系统应提供邮件、声音、SNMP多形式的告警方式。

E.9.5.19 登录防护

支持登陆界面图形验证码，防止管理员账号被暴力破解。

E.9.6 其他安全模块

含攻击规则库 ，可扩展WEBFILTER功能规则库、病毒过滤规则库、无线入侵防御功能等。

E.10 僵木蠕监测

E.10.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.10.2 部署方式

应支持通过分光或者流量镜像方式旁路部署。

E.10.3 性能要求

应满足实际网络环境中需要进行镜像分析的各种木马流量会话连接数之和、且有冗余考虑。

E.10.4 主要功能

E.10.4.1 配置向导

应支持自定义规则配置向导，帮助用户进行配置指引。

E.10.4.2 僵尸主机监测能力

应具备对协议异常、访问异常等行为关联分析。

E.10.4.3 报文取证

应支持将原始僵尸主机行为报文记录，作为电子证据。

E.10.4.4 僵尸主机监测类型

应能够检测僵尸网络、蠕虫病毒、木马等在内在多种僵尸主机攻击类型。

E.10.4.5 木马文件传播监测

应支持对文件类型、大小、传输方向进行监控。

E.10.4.6 疑似样本捕获

除支持对已知木马攻击的监测分析外，还应对疑似木马进行捕获和分析，检验常见可执行文件，将疑似样本进行还原。

E.10.4.7 黑白名单

应支持IP黑白名单、URL黑白名单、文件黑白名单等。

E.10.4.8 旁路阻断

应支持旁路阻断，通过发送 TCP reset 报文阻断连接。

E.10.4.9 防火墙联动

支持与网关类设备联动，阻断攻击连接。

E.10.4.10 日志管理

应支持多种形式的日志存储,如本地存储、外发等。

E.10.4.11 系统易用性

应支持在WEB管理界面直接调用网页命令行窗口，不需要通过串口等方式对设备进行命令行管理。

E.10.4.12 设备监控

应支持对设备的CPU、内存、硬盘利用率等进行监控。

E.10.4.13 实时监测

应支持实时监测统计网络攻击的功能，并以折线图等形式展示一天、一周、一个月等时间内的攻击趋势。

E.10.4.14 规则库

支持应用识别特征库、僵尸主机特征库、木马文件传播特征库单独分开，支持手动、自动、离线升级等。

E.11 APT监测

E.11.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.11.2 工作模式

支持路由、交换、混合、虚拟线工作模式。

E.11.3 性能要求

应满足实际网络环境中需要进行镜像分析的各种APT流量会话连接数之和、且有冗余考虑。

E.11.4 主要功能

E.11.4.1 协议还原

应支持从HTTP、FTP、POP3等协议中还原指定格式文件。

E.11.4.2 文件格式支持

应支持包括Office、WPS、PDF、HTML、压缩包、脚本文件、图片文件等多种默认文件格式。

E.11.4.3 文件静态检测

应支持对Office等文件的静态检测，发现恶意代码。

E.11.4.4 自定义文件

应支持自定义类型的文件检测。

E.11.4.5 白名单功能

应能够对已知的正常样本进行过滤和筛选。

E.11.4.6 手工样本提交

应支持对用户手工上传的文件格式样本进行检测。

E.11.4.7 流量样本检测

应支持对捕获的流量样本文件分析，发现攻击行为。

E.11.4.8 手工样本优先检测

应支持对手工上传样本的优先检测，快速检测。

E.11.4.9 还原文件的加密下载

对系统还原的样本文件，应支持加密后下载。

E.11.4.10 沙箱技术

应支持动态沙箱检测、沙箱逃逸检测、文件行为检测、注册表行为检测、进程行为检测、API调用监测、窗口操作监测、异常处理监测、网络行为监测、恶意宏行为分析、数字签名分析等技术、文件伪装识别、机器学习、流量检测、Web攻击检测等。

E.11.4.11 威胁感知

应支持对实时攻击态势进行地图展示。

E.11.4.12 告警策略

应提供告警策略管理功能，同时支持自定义策略。

E.11.4.13 口令安全策略

应支持对账户进行安全策略配置。

E.12 抗DDoS系统

E.12.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.12.2 工作模式

应支持串接、旁路检测和旁路清洗等模式。

E.12.3 性能参数

E.12.3.1 最大清洗能力

应与实际网络带宽相匹配并对未来业务量增长有足够冗余。

E.12.3.2 最大并发连接数

应满足实际网络环境中各种访问产生的会话连接数之和、且有冗余考虑。

E.12.4 主要功能

E.12.4.1 设备联动

应支持清洗设备、检测设备的联动。

E.12.4.2 双栈支持

应支持IPv4/IPv6双栈方式。

E.12.4.3 系统易用性

应支持基于不同用户，开启不同模式，如企业模式、运营商模式等，方便对设备进行配置。

E.12.4.4 数据采集方式

应支持镜像、分光等方式进行数据采集，

E.12.4.5 业务自学习

应支持业务学习，形成适合用户业务流量的防护基线。

E.12.4.6 流量清洗

应支持网络层清洗、HTTPS协议清洗、HTTP协议清洗、SIP协议清洗、NTP协议清洗、DNS协议清洗。

E.12.4.7 攻击工具防护

应支持常见开源攻击工具和对僵尸工具的防护等。

E.12.4.8 攻击取证

应支持抓包溯源与指纹提取。

E.12.4.9 抓包取证

应支持自动抓包和手动抓包方式。

E.12.4.10 流量牵引

应支持静态路由牵引、动态路由牵引等。

E.12.4.11 流量回注

应支持多种流量回注方式。

E.12.4.12 配置向导

应提供配置向导功能，使设备上线更加便捷简易。

E.12.4.13 日志存储

应支持日志本地存储和外发。

E.12.4.14 网络分析

应支持威胁分析、流量分析、连接分析等网络分析功能。

E.12.4.15 实时监控

应支持监控展示DIY，根据客户需求选择指定内容展示。

E.12.4.16 统一管理

应支持多设备集中管理，日志收集，状态监控，策略下发等功能。

E.12.4.17 防护对象自学习

应支持自动学习防护对象IP，添加到默认防护对象，不需要手动一个个添加。

E.12.4.18 设备告警

应支持对设备硬件状态、系统状态等进行告警。

E.12.4.19 告警方式

应支持短信、邮件、声音告警等方式。

E.12.4.20 系统诊断

应支持多种网络通断性检测方式。

E.13 网页防篡改

E.13.1 运行环境支持

应支持在windows、Unix、Linux、Solaris等环境下运行。

E.13.2 主要功能

E.13.2.1 防篡改

应支持各类网页文件的保护，如静态、动态网页等。

E.13.2.2 文件夹保护

应支持对指定文件夹以及子文件夹的保护。

E.13.2.3 篡改恢复

在文件被篡改的情况下，能快速恢复被篡改页面。

E.13.2.4 断线检测

应支持在断线情况下对网页文件目录的防护功能。

E.13.2.5 进程管理

应提供进程黑白名单设置，支持服务监控。

E.13.2.6 文件同步

应支持手工文件同步、手工文件备份等。

E.13.2.7 动态防护

应支持添加许可路径，排除父目录下某些子目录的保护。

E.13.2.8 同步功能

应支持跨平台自动同步、一对多自动同步等方式。

E.13.2.9 服务器监控

应支持服务器性能实时监控，如内存、CPU占用率等。

E.13.2.10 用户管理

应支持多用户权限分级,各个用户拥有相应的权限。

E.13.2.11 通信保护

系统各个模块、进程之间的通讯应采用加密传输方式。

E.13.2.12 卸载保护

程序卸载时需要提供管理员权限，防止恶意卸载。

E.13.2.13 报警方式

应支持声音报警、邮件报警、弹窗报警等方式。

E.13.2.14 系统日志

应支持对用户操作、文件操作和修改等进行完整日志记录，支持日志导出等。

E.14 负载均衡设备

E.14.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.14.2 部署模式

支持串行、旁路、三角传输等部署模式。

E.14.3 高可用性

应支持双机热备，链路聚合等功能。

E.14.4 性能参数

E.14.4.1 整机吞吐量

应与实际业务带宽相匹配并对未来业务量增长有足够冗余。

E.14.4.2 最大并发连接数

应满足实际网络环境中各种会话连接数之和、且有冗余考虑。

E.14.5 基本功能

E.14.5.1 功能支持

应支持链路、服务器、全局负载和链路过载保护。

E.14.5.2 应用路由

应支持基于应用进行链路选择，保证链路按需所用。

E.14.5.3 服务器负载均衡

应提供L4-L7层内容交换服务器负载功能。

E.14.5.4 服务器健康检查

应采用主动和被动健康检查相结合的方式。

E.14.5.5 服务器过载保护

针对服务器负载状态进行保护，支持服务器温暖上线和软关机、平滑退出功能。

E.14.5.6 协议优化

应支持TCP连接复用、WEB压缩功能和WEB缓存加速功能。

E.14.5.7 页面加速

应提供CSS加速、JavaScript加速和HTML加速功能。

E.14.5.8 页面防护

应支持基于五元组进行访问控制。

E.14.5.9 Web防护

应支持SQL注入防护、XSS攻击防护、WEBSHELL防护、暴力工具防护、网页挂马防护、IP黑白名单等。

E.14.5.10 数据库安全

应检查访问数据库的权限，杜绝非授权用户的访问。

E.14.5.11 抗DDoS

应提供L4-L7层抗DDoS攻击功能。

E.14.5.12 漏洞扫描

应提供漏洞扫描功能，发现服务器操作系统漏洞。

E.14.5.13 流量管理

应支持链路的上下行带宽控制。

E.14.5.14 决策分析

应记录用户访问行为并进行来源分析。

E.14.5.15 系统管理与配置

支持WEB界面与命令行管理，提供配置向导。

E.14.5.16 设备告警

应支持邮件、声音等告警方式。

E.15 上网行为管理

E.15.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.15.2 部署模式

应支持路由模式，旁路模式、网桥模式、混合模式部署。

E.15.3 高可用性

应支持双机热备，链路聚合等功能。

E.15.4 性能参数

E.15.4.1 整机吞吐量

应与实际业务访问互联网带宽相匹配并对未来增长有足够冗余。

E.15.4.2 最大用户数

应满足实际网络环境中用户数之和、且有冗余考虑。

E.15.5 基本功能

E.15.5.1 即插即用

应支持即插即用功能，快速部署。

E.15.5.2 网络功能

应支持静态、动态、策略路由。

E.15.5.3 链路健康检查

应支持多种链路健康检查算法。

E.15.5.4 排障工具

应提供排障及抓包工具，便于管理员排查故障。

E.15.5.5 集中管理

应支持分布式部署，通过集中管理平台，实现统一维护。

E.15.5.6 服务监控

应提供服务趋势图，快速定位使用对应服务的用户。

E.15.5.7 用户监控

应提供用户流量使用情况，支持下线用户或修改带宽等。

E.15.5.8 用户有效期

应支持多种用户身份的有效期设置。

E.15.5.9 临时账号

应支持临时账号自动申请功能，方便临时用户使用。

E.15.5.10 认证方式

应支持本地认证和第三方认证。

E.15.5.11 规则库

应提供URL库和应用识别库，并保持定期更新。

E.15.5.12 流量过滤

应支持邮件过滤、关键字过滤等技术。

E.15.5.13 发帖管理

应支持常见论坛发帖控制。

E.15.5.14 网页附件管理

应支持常见网盘的文件过滤。

E.15.5.15 网络防共享

应支持禁止私接无线路由器。

E.15.5.16 移动终端管理

应支持无线环境下的移动终端接入控制。

E.15.5.17 网监平台

应支持与网监平台对接并按照网监要求上传日志。

E.15.5.18 网络审计

应支持发帖行为，telnet、http、ftp上传下载审计。

E.15.5.19 个人统计分析

应支持基于个人的所有行为监控报表。

E.16 网络流量分析系统

E.16.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.16.2 设备性能

建议根据实际网络环境中需要进行分析的各类镜像流量之和选型。

E.16.3 部署模式

支持旁路部署、分布式部署等。

E.16.4 主要功能

E.16.4.1 网络流量透视

支持实时监控流量，支持动态图实时多维度展示。

E.16.4.2 流量关联分析

支持对网络流量的应用、用户、等数据相互关联。

E.16.4.3 业务识别与管理

支持识别P2P、炒股、网游等主流网络应用。

E.16.4.4 业务性能分析

支持对HTTP网页访问服务的综合评价分析。

E.16.4.5 业务实时监控

支持http业务监控和非加密页面访问行为页面还原。

E.16.4.6 网络性能实时监控

支持对TCP连接信息分析；支持安全事件自动触发原始数据报文保存；支持可疑文件还原。

E.16.4.7 流量控制与过滤

支持带宽控制，对网络流量进行实时在线控制。

E.16.4.8 支持黑白名单

添加黑白名单指定IP地址或用户名,白名单用户不受任何流控策略影响,黑名单用户禁止任何通信。

E.16.4.9 数据包过滤

用户根据需要下发过滤策略，监控系统为用户提供过滤掉不关心的数据的功能，只输出用户想要的那部分数据。

E.16.4.10 告警与预警

支持基准线告警，对于系统所能获得的各种指标进行建模，建立基准线，实时对网络、用户、流量和业务的异常表现进行主动告警和预警，支持短信、邮件等告警方式。

E.16.4.11 多元数据采集与开放共享

支持分布式数据采集、存储、本地缓存，支持百万并发业务流记录的存储，支持多层次、多粒度的网络流量匹配和处理，支持第三方服务和共享接口，支持实时、历史数据的服务与共享。

E.16.4.12 应用特征库

支持在线和离线应用特征库升级。

E.17 单向网闸

E.17.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.17.2 设备性能

建议根据实际网络环境中需要单向传输的网络流量大小进行选型，并有冗余考虑。

E.17.3 工作模式

支持透明、路由、代理模式等。

E.17.4 产品架构

由接收端、发送端、专有单向光隔离硬件三部分组成。

E.17.5 安全体系结构

以光信号物理单向传输隔离的方式，有效地隔断内外网络间的反向物理连接，保证数据信号的单向无反馈传输。

E.17.6 安全操作系统

安全操作系统内核基于光隔离技术单向不可编程。

E.17.7 主要功能

E.17.7.1 单向文件传输

支持自动从外网向内网服务器进行单向的文件摆渡。

E.17.7.2 客户端支持

支持客户端和无客户端方式，支持windows和Linux客户端，无客户端方式支持FTP和SMB协议。

E.17.7.3 用户权限

支持数据标记级别的用户权限分配，如高级别用户可以下载、查看低级别用户的文件，低级别无权查看高级别用户的文件。

E.17.7.4 私有目录

支持为每个用户分配独立的私有目录，用户可选择将文件上传至公共区还是个人私有区。

E.17.7.5 单向邮件传输

支持自动从外网向内网进行单向的邮件信息摆渡。

E.17.7.6 邮件过滤

支持邮件主题和正文内容过滤，支持邮件附件过滤，支持邮件附件大小和附件格式黑白名单控制。

E.17.7.7 数据库同步

支持自动把外网数据库记录同步到内网数据库服务器，支持数据库实时同步或定时同步策略。

E.17.7.8 数据库支持

支持多种国内国外主流数据库的同步。

E.17.7.9 冲突检测

支持数据冲突检测机制，当发生冲突时灵活处理。

E.17.7.10 组播代理支持

支持组播代理功能，可穿透三层交换机进行部署。

E.17.7.11 数据包加冗传输

支持多次传输同一数据包，降低数据包丢失的概率，传输次数可自定义。

E.17.7.12 TCP双向联动

支持两台光闸联动，实现标准TCP双向业务交互，对接主流视频厂商如海康、大华的视频平台，实现视频监控应用的安全传输。

E.17.7.13 访问控制

双重访问控制，内外网端的访问控制规则完全独立。

E.17.7.14 防病毒功能

内置病毒库对经过光闸的文件数据进行病毒检测。

E.17.7.15 文件管理

支持光闸内置安全存储空间管理，可手动查看和删除发送端和接收端安全存储区的文件内容。

E.17.7.16 外挂存储

支持外挂网络存储，可直接挂载用户网络中的存储设备。

E.17.7.17 配置管理

采用发送端和接收端各自独立配置的管理模式，不允许采用数据通讯口进行管理。

E.17.7.18 设备监控

支持实时查看发送端和接收端CPU、内存以及存储使用率。

E.17.7.19 协议支持

支持双机热备，支持SNMP协议，与标准网管平台兼容。

E.17.7.20 网络诊断工具

支持ping、traceroute、TCP端口连接等诊断工具。

E.18 双向网闸

E.18.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.18.2 设备性能

建议根据实际网络环境中需要传输的网络流量大小进行选型，并有冗余考虑。

E.18.3 工作模式

支持透明、路由、代理模式等。

E.18.4 产品架构

内外端机之间采用专用硬件和协议进行连接，不可编程。

E.18.5 安全防护

内置IDS特征库，集成抗DDOS和病毒查杀功能。

E.18.6 主要功能

E.18.6.1 安全上网功能

支持WEB访问，支持HTTP协议应用的各种指令控制。

E.18.6.2 内容过滤

支持关键字过滤、文件过滤等。

E.18.6.3 安全邮件功能

提供安全的邮件访问，支持POP3、SMTP协议。

E.18.6.4 文件同步

支持有客户端和无客户端方式，支持多种通信协议。

E.18.6.5 数据库同步

支持有客户端和无客户端方式，支持多种主流数据库。

E.18.6.6 视频监控

提供视频代理功能，兼容主流视频传输及控制协议，支持对平台级联通信过程中的视频信令进行黑白名单控制。

E.18.6.7 组播应用

支持多任务的组播代理功能，可穿透三层交换机部署。

E.18.6.8 自定义功能

支持自定义的TCP、UDP协议，无需二次修改开发。

E.18.6.9 强制认证功能

支持强制认证，可开启或者禁用对用户的强制认证。

E.18.6.10 内容过滤

支持文件类型黑白名单过滤,关键字过滤等。

E.18.6.11 设备监控

可以实时的了解到设备的CPU、内存、并发连接等。

E.18.6.12 策略备份

支持设备策略的一键导入导出，支持定期远程备份。

E.18.6.13 日志审计

支持系统日志、管理日志、访问日志等，支持日志本地存储和日志外发。

E.18.6.14 双机热备

支持双机热备，备机不需要二次配置自动学习。

E.19 工控网闸

E.19.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.19.2 设备性能

建议根据实际工控网络中需要传输的网络流量大小和网络时延进行选型，并有冗余考虑。

E.19.3 工作模式

支持透明、路由、代理模式等。

E.19.4 产品架构

内外端机之间采用专用硬件和协议进行连接，不可编程。

E.19.5 安全防护

内置IDS特征库，集成抗DDOS和病毒查杀功能。

E.19.6 主要功能

E.19.6.1 安全上网功能

支持WEB访问，支持HTTP协议应用的各种指令控制。

E.19.6.2 内容过滤

支持关键字过滤、文件过滤等。

E.19.6.3 安全邮件功能

提供安全的邮件访问，支持POP3、SMTP协议。

E.19.6.4 OPC工控协议支持

支持DCS/SCADA网络与传统网络之间的OPC应用数据传输，支持同步、异步监测数据的传输，支持OPC读写指令控制，支持设置OPC工控应用允许通信的时间。

E.19.6.5 Modbus工控支持

支持DCS/SCADA网络与传统网络之间的Modbus应用数据传输，支持Modbus控制协议解析及内部命令控制，支持协议功能码控制，例如读写线圈、读写寄存器的控制。

E.19.6.6 WINCC工控支持

支持DCS/SCADA网络与传统网络之间西门子WINCC应用数据传输，支持西门子控制协议解析及内部命令控制，支持协议功能码控制，例如只允许读取，不允许写入控制操作。

E.19.6.7 TCP单向无反馈

支持TCP应用层数据单向传输控制，保证TCP应用数据0反馈，以满足二次防护的安全性需求。

E.19.6.8 文件同步

支持有客户端和无客户端方式，支持多种通信协议。

E.19.6.9 数据库同步

支持有客户端和无客户端方式，支持多种主流数据库。

E.19.6.10 视频监控

提供视频代理功能，兼容主流视频传输及控制协议，支持对平台级联通信过程中的视频信令进行黑白名单控制。

E.19.6.11 组播应用

支持多任务的组播代理功能，可穿透三层交换机部署。

E.19.6.12 自定义功能

支持自定义的TCP、UDP协议，无需二次修改开发。

E.19.6.13 强制认证功能

支持强制认证，可开启或者禁用对用户的强制认证。

E.19.6.14 内容过滤

支持文件类型黑白名单过滤,关键字过滤等。

E.19.6.15 设备监控

可以实时的了解到设备的CPU、内存、并发连接等。

E.19.6.16 策略备份

支持设备策略的一键导入导出，支持定期远程备份。

E.19.6.17 日志审计

支持系统日志、管理日志、访问日志等，支持日志本地存储和日志外发。

E.19.6.18 双机热备

支持双机热备，备机不需要二次配置自动学习。

E.20 网络审计

E.20.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.20.2 设备性能

建议根据实际网络环境中需要进行审计的各类镜像流量之和选型，并有冗余考虑。

E.20.3 部署方式

支持单点、多点、多级管理模式 ；采用B/S管理方式，不需要单独的管理设备。

E.20.4 系统要求

采用专用安全操作系统，支持双操作系统，当主系统故障时可用备系统恢复。

E.20.5 监听接口授权

无需额外购买接口审计授权，默认所有接口可以审计。

E.20.6 主要功能

E.20.6.1 实名审计

支持802.1x,PPPoE,AD等环境下终端IP地址和用户实名信息或主机信息绑定显示，可显示在线用户的PPPoE账号和AD域用户等信息。

E.20.6.2 HTTP审计

支持对HTTP协议进行审计，审计内容包括http请求类型、http响应类型、请求文件、请求参数等。

E.20.6.3 应用协议识别

支持识别多类应用协议，支持把应用协议分组审计。

E.20.6.4 协议审计

支持FTP、Telnet、即时通讯等协议以及邮件审计。

E.20.6.5 攻击检测

支持对入侵行为的管理和侦听，对攻击信息详细审计。

E.20.6.6 流量分析

支持流量趋势分析，对各类协议进行统计和多条件分析。

E.20.6.7 NetFlow分析

支持分析其他设备发送的NetFlow，支持v5/v9版本。

E.20.6.8 攻击阻断

支持旁路攻击阻断，支持与防火墙联动进行阻断。

E.20.6.9 登录锁定

可自定义用户名/密码尝试次数和登录锁定时间。

E.20.6.10 一体化

审计、解析、报警、存储均在一台设备上实现。

E.20.6.11 授权扩张

通过扩展授权许可，可在网络审计上实现数据库审计。

E.20.6.12 IPv6支持

支持IPV6环境部署和IPV6环境下的网络审计。

E.21 数据库审计

E.21.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.21.2 设备性能

建议根据实际网络环境中需要进行分析的各类数据库镜像流量之和选型，并有冗余考虑。

E.21.3 部署方式

支持单点、多点、多级管理模式 ；采用B/S管理方式，不需要单独的管理设备。

E.21.4 系统要求

采用专用硬件平台（非Windows平台）和专用安全操作系统，支持双操作系统，当常用系统出现故障可以使用备用系统恢复。

E.21.5 监听接口授权

无需额外购买接口审计授权，默认所有接口可以审计。

E.21.6 主要功能

E.21.6.1 数据库支持

支持审计国内国外各类主流数据库系统，如ORACLE、SQL Server、Cache、Mongo dB等。

E.21.6.2 数据库审计

支持对数据库DML、DCL、DDL语句的审计，可审计的信息如源地址、目的地址、时间等。

E.21.6.3 审计查询

支持按数据库名、表名、字段名等作为查询和统计条件。

E.21.6.4 数据库分析

支持数据库事件进行潜在危害分析，实时告知管理员。

E.21.6.5 数据库防护

支持对针对数据库的攻击行为，数据库暴力破解进行审计并实时报警。

E.21.6.6 审计关联

支持中间件环境下的SQL语句关联到HTTP操作，HTTP操作关联到HTTP-ID，实现中间件环境下的审计追溯。

E.21.6.7 登录锁定

可自定义用户名/密码尝试次数和登录锁定时间。

E.21.6.8 一体化

审计、解析、报警、存储均在一台设备上实现。

E.21.6.9 授权扩展

通过扩展授权许可，可在数据库审计上实现网络审计。

E.21.6.10 IPv6支持

支持IPV6环境部署和IPV6环境下的网络审计。

E.22 工控审计

E.22.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.22.2 设备性能

建议根据实际工控网络中需要进行分析的各类镜像流量之和选型，并有冗余考虑。

E.22.3 部署方式

支持单点、多点、多级管理模式。

E.22.4 系统要求

采用专用硬件平台（非Windows平台）和安全操作系统。

E.22.5 审计接口授权

无需额外购买接口审计授权，默认所有接口可以审计。

E.22.6 主要功能

E.22.6.1 设备监控

支持监测CPU状态、内存状态、硬盘状态等信息。

E.22.6.2 智能学习

支持根据网络流量自动生成通信模型，形成安全基线。

E.22.6.3 白名单对比

支持对当前通信行为与白名单对比，对偏离白名单的行为进行告警。

E.22.6.4 工控协议支持

支持Modbus TCP、S7、OPCUA、OPCDA、CIP、IEC104等常用协议实现PDU类型和功能码操作、操作地址、值的解析。

E.22.6.5 协议支持开关

支持开启或关闭支持的协议模块，优化产品性能。

E.22.6.6 安全时间回溯

支持通过事件详情查看告警事件相关信息及原始通信内容，实现事件安全回溯。

E.22.6.7 检测规则调整

可对规则添加、删除和修改，包括工控设备和网络设备的漏洞特征信息、已知攻击特征等。

E.22.6.8 审计报告

支持通过端口号、协议类型等生成报告，并邮件发送。

E.22.6.9 实时告警

支持流量异常、未知设备发现、通信异常、通信数据异常等威胁事件的实时告警功能。

E.22.6.10 关键业务检测

支持在设定的时间内，某IP报文为零时进行告警。

E.22.6.11 安全状态评估

支持按威胁程度划分告警事件、对被监测设备进行设备安全状态评分。

E.23 网络安全准入

E.23.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.23.2 设备性能

建议根据实际网络环境中需要进行的准入认证的用户数进行选型，并有冗余考虑。

E.23.3 部署方式

支持旁路或串联部署。

E.23.4 系统要求

采用专用硬件平台（非Windows平台）和安全操作系统。

E.23.5 主要功能

E.23.5.1 准入模式

支持802.1X、Portal、透明网关、策略路由等多种准入模式，单设备支持混合准入模式。

E.23.5.2 认证方式

支持客户端认证、手机短信认证等。

E.23.5.3 设备可靠性

支持硬件BYPASS功能，支持双操作系统冷备、双机热备，单机模式下的系统逃生工具等。

E.23.5.4 客户端兼容

支持windows XP、windows7/8/8.1/10/server2008操作系统；浏览器：浏览器插件兼容IE8及以上版本。

E.23.5.5 终端检查

支持检查入网终端IP、终端MAC、用户名等多要素信息。

E.23.5.6 访客管理

访客接入由固定用户协助注册、账户创建等操作，提供入网有效期，可设置在网时限。

E.23.5.7 黑白名单

设置黑/白名单终端IP、MAC等信息，进行入网控制。

E.23.5.8 终端健康检查

支持检查项自定义，包括防火墙、杀毒软件检查等。

E.23.5.9 终端外设监控

可对终端外设实施启停控制，设置例外项等。

E.23.5.10 非法外联监控

支持通过http、telnet、ping等方式检测主机违规外联行为，给予相应的违规处理。

E.23.5.11 资产管理

可管理不同类型入网资产，支持资产发现，资产审批。

E.23.5.12 日志内容

提供终端解绑、资产登录、终端认证、健康检查等信息。

E.23.5.13 认证界面自定义

支持系统界面与登录界面LOGO的自定义导入。

E.24 综合VPN网关

E.24.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.24.2 设备性能

建议根据实际网络环境选型。

E.24.3 部署方式

支持透明、路由、混合模式。

E.24.4 系统要求

采用专用硬件平台（非Windows平台）和安全操作系统。

E.24.5 性能要求

E.24.5.1 IPSEC隧道数

应满足实际网络环境中需要建立的虚拟隧道数之和、且有冗余考虑。

E.24.5.2 IPSEC吞吐率

应满足实际网络环境接入的IPSEC VPN会话之和，并有冗余考虑。

E.24.5.3 SSL用户数

应满足实际网络环境中需要接入的用户数目，并有冗余考虑。

E.24.5.4 SSL吞吐率

应满足实际网络环境接入的SSL VPN会话之和，并有冗余考虑。

E.24.6 主要功能

E.24.6.1 智能选路

支持多线路的智能选路，支持多线路隧道的负载均衡和备份。

E.24.6.2 IPv6支持

支持IPv6网络环境下的运行。

E.24.6.3 用户管理

支持IPSEC与SSL使用同一套用户认证系统，方便管理。

E.24.6.4 个性化界面

支持用户资源界面个性化，可选择导入自定义界面。

E.24.6.5 数字证书

支持内置CA，可为其他设备或移动用户签发证书。

E.24.6.6 VPN支持

支持IPSEC VPN、SSL VPN、GRE、PPTP等。

E.24.6.7 转发模式

支持WEB转发、端口转发、全网接入模式等。

E.24.6.8 认证授权

支持短信、动态令牌、硬件特征码、图形码认证。

E.24.6.9 第三方认证

支持如RADIUS、TACACS、LDAP等第三方认证方式。

E.24.6.10 可信接入

支持接入主机的安全检查。

E.24.6.11 流量管理

支持根据IP、协议、角色、接口、时间等定义带宽分配策略，支持最小保证带宽和最大限制带宽。

E.24.6.12 高可用性

支持双机热备、负载均衡、连接保护模式。

E.24.6.13 系统管理

支持管理员分权管理，不同管理员管理不同的功能模块。

E.24.6.14 日志传输

支持Welf、Syslog等多种日志格式的输出。

E.24.6.15 设备配置

支持WEB图形配置、命令行配置。

E.24.6.16 系统升级

支持双系统引导，支持TFTP、网页等方式升级。

E.25 国密加密机

E.25.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.25.2 设备性能

建议根据实际网络环境选型。

E.25.3 部署方式

支持透明、路由、混合模式。

E.25.4 系统要求

采用专用硬件平台（非Windows平台）和安全操作系统。

E.25.5 性能要求

E.25.5.1 IPSEC隧道数

应满足实际网络环境中需要建立的虚拟隧道数之和、且有冗余考虑。

E.25.5.2 IPSEC吞吐率

应满足实际网络环境接入的IPSEC VPN会话之和，并有冗余考虑。

E.25.5.3 SSL用户数

应满足实际网络环境中需要接入的用户数目，并有冗余考虑。

E.25.5.4 SSL吞吐率

应满足实际网络环境接入的SSL VPN会话之和，并有冗余考虑。

E.25.6 主要功能

E.25.6.1 智能选路

支持多线路源路返回，支持多机多线路隧道的负载均衡和备份。

E.25.6.2 IPv6支持

支持IPv6网络环境下的运行。

E.25.6.3 用户管理

支持IPSEC与SSL使用同一套用户认证系统，方便管理。

E.25.6.4 个性化界面

支持用户资源界面个性化，可选择导入自定义界面。

E.25.6.5 数字证书

支持内置CA，可为其他设备或移动用户签发证书。

E.25.6.6 SSL VPN规范性

符合国密局制定的《SSL VPN技术规范》，支持国家商用密码算法SM1、SM2、SM3、SM4。

E.25.6.7 转发模式

支持WEB转发、端口转发、全网接入模式等。

E.25.6.8 认证授权

支持短信、动态令牌、硬件特征码、图形码认证。

E.25.6.9 第三方认证

支持如RADIUS、TACACS、LDAP等第三方认证方式。

E.25.6.10 可信接入

支持接入主机的安全检查。

E.25.6.11 IPSEC VPN规范性

符合国密局制定的《IPSEC VPN技术规范》，支持国家商用密码算法SM1、SM2、SM3、SM4。

E.25.6.12 流量管理

支持根据IP、协议、角色、接口、时间等定义带宽分配策略，支持最小保证带宽和最大限制带宽。

E.25.6.13 高可用性

支持双机热备、负载均衡、连接保护模式。

E.25.6.14 系统管理

支持管理员分权，不同管理员管理不同的功能模块。

E.25.6.15 日志传输

支持Welf、Syslog等多种日志格式的输出。

E.25.6.16 设备配置

支持WEB图形配置、命令行配置。

E.25.6.17 系统升级

支持双系统引导，支持TFTP、网页等方式升级。

E.26 移动终端安全管理平台

E.26.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.26.2 设备性能

建议根据实际需要管理的移动终端数量进行选型，并有冗余考虑。

E.26.3 部署方式

旁路部署。

E.26.4 系统要求

采用专用硬件平台（非Windows平台）和安全操作系统。

E.26.5 主要功能

E.26.5.1 设备分组管理

支持按照设备平台、类型进行分组，下发不同权限。

E.26.5.2 设备信息获取

支持获取移动终端的系统版本、设备型号等信息。

E.26.5.3 用户管理

支持单一用户绑定多台移动终端，绑定数量可限定。

E.26.5.4 分类搜索

支持按照设备类型，设备状态、操作平台进行分类搜索。

E.26.5.5 设备定位

支持设备定位，在北斗/GPS模式下误差不超过20米。

E.26.5.6 病毒查杀

支持服务器端、客户端的病毒查杀、准入机制。

E.26.5.7 状态统计

支持终端注册状态、告警事件、系统版本、操作平台百分比、内存用量等详细信息的图表统计。

E.26.5.8 应用市场

支持企业自有及第三方Android、iOS应用自有APP市场。

E.26.5.9 APP管理

支持APP黑白名单，APP加固功能、APP漏洞扫描功能。

E.26.5.10 文档管理

支持根据用户权限设置文档浏览权限。

E.26.5.11 日志审计

支持用户信息、设备信息、报警信息、应用信息、失联信息等的完整日志审计功能。

E.26.5.12 App store同步

可与苹果“App store”发布的官方应用进行同步，针对自有应用进行安装情况统计。

E.26.5.13 静默卸载

支持静默卸载功能，被管设备在网络畅通的情况下10秒内接收到卸载命令开始卸载。

E.26.5.14 操作权限管控

支持IOS/ANDROID系统常用的配置，可限制设备的操作权限（禁用摄像头、蓝牙、WIFI、剪切板等）、可连接WIFI、密码策略、WIFI黑白名单、VPN等内容。

E.26.5.15 安卓防卸载

支持安卓客户端防卸载功能，防止用户强制脱离管控。

E.26.5.16 终端壁纸设定

支持安卓设备背景壁纸统一设定。

E.26.5.17 即时通讯

支持终端加密点对点即时通信工具，消息传输过程通中过消息内容采用非对称密钥加密，服务器不存储消息内容。传输工具有防截屏功能，支持消息限时浏览、阅后即焚。

E.26.5.18 移动杀毒

支持移动杀毒客户端，对终端设备病毒查杀。

E.26.5.19 移动门户

支持在移动门户中集中展示企业APP，系统中无法找到企业应用，登陆移动门户密码认证支持Touch ID认证方式。

E.26.5.20 深度整合

支持与SSL-VPN深入整合，支持用户无感知接入SSL-VPN。

E.27 移动APP扫描加固系统

E.27.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.27.2 设备性能

建议根据实际需要监测的APP数量进行选型。

E.27.3 部署方式

旁路部署。

E.27.4 系统要求

具备自主知识产权，稳定可靠。

E.27.5 主要功能

E.27.5.1 安全库

包含恶意URL库、恶意APP库、APP漏洞库、恶意行为库等。

E.27.5.2 多层检测

覆盖代码、组件、文件和数据存储多个层面。

E.27.5.3 安全加固

具有防篡改、注入、逆向破解等，兼容性强。

E.27.5.4 渠道监测

覆盖国内外APP发布渠道，及时响应。

E.27.5.5 专业报告

检测报告精准问题定位，详细解决方案。

E.27.5.6 多层加固效果校检

覆盖代码、组件、文件和数据存储多个层面。

E.27.5.7 身份鉴别

提供登录控制模块核实用户身份，防止非法入侵。

E.27.5.8 通讯安全

对在通信过程中的整个报文或会话过程进行加密。

E.27.5.9 任务流程

支持一键上传APP安装包，提交待测APP等待任务完成，支持显示检测状态，如正在进行、任务完成、任务失败等。

E.27.5.10 结果反馈

预留用户修改检测结果功能，管理员可审批修改申请。

E.27.5.11 审计日志

记录用户登录退出、重要操、设备自身日志等内容。

E.27.5.12 配置安全

能够扫描APP客户端XML配置文件，识别不安全配置。

E.27.5.13 通信安全

能够对被安装包进行壳分析、逆向分析、数据流分析等。

E.27.5.14 漏洞检测

能够对被测系统客户端安装包进行漏洞检测。

E.27.5.15 行为分析

能够对被测系统客户端安装包进行行为分析。

E.27.5.16 评分标准

参考国家、行业或者地方的APP安全检测标准给出评分。

E.27.5.17 加固功能

支持核心代码保护，支持反调试保护功能，支持对应用数据文件加密，支持应用文件防篡改等。

E.27.5.18 兼容性

适配主要的手机厂家的移动终端。

E.27.5.19 监测渠道

监测Android应用发布渠道不少于50家。

E.27.5.20 盗版识别

至少根据不少于两种特征识别盗版应用。

E.28 系统漏洞

E.28.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.28.2 设备性能

建议根据需要并发扫描的IP数量和并发任务数量进行选型。

E.28.3 部署方式

旁路部署。

E.28.4 系统要求

采用经过系统加固的专有操作系统。

E.28.5 主要功能

E.28.5.1 防暴力破解

用户多次登录失败时，自动锁定登录IP。

E.28.5.2 网络支持

支持IPv4/IPv6双协议栈地址场景漏洞扫描。

E.28.5.3 资产管理

支持资产自动发现功能，支持手动添加资产。

E.28.5.4 漏洞库标准

漏洞库应具备CVE、CNNVD、CNVD等编号。

E.28.5.5 扫描信息

包括主机信息、用户信息、服务信息、漏洞信息等内容。

E.28.5.6 兼容性

支持Windows系列、苹果操作系统、Linux、网络设备、移动终端Android、apple、BlackBerry、虚拟化平台等的漏洞扫描。

E.28.5.7 安全性检查

支持对扫描对象脆弱性的全面检查，如安全补丁、口令、服务配置等。

E.28.5.8 扫描策略

可以并行地检查多个被评估的系统，能够提供扫描策略定制，可以保证扫描的安全性，不影响应用系统和网络业务的正常运行。

E.28.5.9 无限IP扫描

硬件性能足够的情况下，提供无限IP漏洞扫描能力。

E.28.5.10 扫描功能

支持主机存活探测，支持弱口令扫描。

E.28.5.11 告警方式

支持扫描完成后进行SNMP trap告警、短信告警等。

E.28.5.12 报表功能

报告具有漏洞描述和安全修补方案建议，并提供相关的技术站点以供管理员参考。

E.28.5.13 威胁分级

应可对安全的威胁程度分级，形成风险趋势分析报表。

E.28.5.14 报告查询

支持按照任务、主机、资产等多种方式查询。

E.28.5.15 结果对比

支持同一任务的两次扫描结果对比，清晰明了的展示出漏洞状态的变更情况。

E.28.5.16 规则库升级

支持自动/手动/本地升级/代理服务器等升级方式。

E.29 数据库漏扫

E.29.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.29.2 设备性能

建议根据需要并发扫描的数据库数量和并发任务数量进行选型。

E.29.3 部署方式

旁路部署。

E.29.4 系统要求

采用经过系统加固的专有操作系统。

E.29.5 主要功能

E.29.5.1 防暴力破解

用户多次登录失败时，自动锁定登录IP。

E.29.5.2 网络支持

支持IPv4/IPv6双协议栈地址场景漏洞扫描。

E.29.5.3 资产管理

支持资产自动发现功能，支持手动添加资产。

E.29.5.4 漏洞库标准

漏洞库应具备CVE、CNNVD、CNVD等编号。

E.29.5.5 扫描信息

包括主机信息、用户信息、服务信息、漏洞信息等内容。

E.29.5.6 支持的数据库类型

支持Oracle、SQL Server、MySQL、Sybase、DB2、Informix、Dameng和King Base，等的漏洞扫描。

E.29.5.7 安全性检查

支持对扫描对象脆弱性的全面检查，如安全补丁、口令、服务配置等。

E.29.5.8 扫描策略

可以并行地检查多个被评估的系统，能够提供扫描策略定制，可以保证扫描的安全性，不影响应用系统和网络业务的正常运行。

E.29.5.9 无限IP扫描

硬件性能足够的情况下，提供无限IP漏洞扫描能力。

E.29.5.10 扫描功能

支持主机存活探测，支持弱口令扫描。

E.29.5.11 告警方式

支持扫描完成后进行SNMP trap告警、短信告警等。

E.29.5.12 报表功能

报告具有漏洞描述和安全修补方案建议，并提供相关的技术站点以供管理员参考。

E.29.5.13 威胁分级

应可对安全的威胁程度分级，形成风险趋势分析报表。

E.29.5.14 报告查询

支持按照任务、主机、资产等多种方式查询。

E.29.5.15 结果对比

支持同一任务的两次扫描结果对比，清晰明了的展示出漏洞状态的变更情况。

E.29.5.16 规则库升级

支持自动/手动/本地升级/代理服务器等升级方式。

E.30 Web漏扫

E.30.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.30.2 设备性能

建议根据需要并发扫描的Web服务数量和并发任务数量进行选型。

E.30.3 部署方式

旁路部署。

E.30.4 系统要求

采用经过系统加固的专有操作系统。

E.30.5 主要功能

E.30.5.1 防暴力破解

用户多次登录失败时，自动锁定登录IP。

E.30.5.2 网络支持

支持IPv4/IPv6双协议栈地址场景漏洞扫描。

E.30.5.3 资产管理

支持资产自动发现功能，支持手动添加资产。

E.30.5.4 漏洞库标准

漏洞库应具备CVE、CNNVD、CNVD等编号。

E.30.5.5 扫描信息

包括主机信息、用户信息、服务信息、漏洞信息等内容。

E.30.5.6 Web漏洞库

按照国际权威安全组织OWASP标准。

E.30.5.7 Web漏扫

支持暗链检测、网站木马检测，支持登录认证，支持网站架构实时展示，支持目录树形式显示漏洞分布。

E.30.5.8 漏洞展示

支持历次漏洞结果列表展示，并可以查看某一次结果的详细内容，漏洞结果展示支持详细的HTTP请求头内容，支持漏洞验证功能。

E.30.5.9 安全性检查

支持对扫描对象脆弱性的全面检查，如安全补丁、口令、服务配置等。

E.30.5.10 扫描策略

可以并行地检查多个被评估的系统，能够提供扫描策略定制，可以保证扫描的安全性，不影响应用系统和网络业务的正常运行。

E.30.5.11 扫描功能

支持主机存活探测，支持弱口令扫描。

E.30.5.12 告警方式

支持扫描完成后进行SNMP trap告警、短信告警等。

E.30.5.13 报表功能

报告具有漏洞描述和安全修补方案建议，并提供相关的技术站点以供管理员参考。

E.30.5.14 威胁分级

应可对安全的威胁程度分级，形成风险趋势分析报表。

E.30.5.15 报告查询

支持按照任务、主机、资产等多种方式查询。

E.30.5.16 结果对比

支持同一任务的两次扫描结果对比，清晰明了的展示出漏洞状态的变更情况。

E.30.5.17 规则库升级

支持自动/手动/本地升级/代理服务器等升级方式。

E.31 工控漏洞

E.31.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.31.2 设备性能

建议根据需要并发扫描的工控设备数量和并发任务数量进行选型。

E.31.3 部署方式

旁路部署。

E.31.4 网络支持

支持IPv4/IPv6双协议栈场景下的漏洞扫描。

E.31.5 系统要求

采用经过安全加固的操作系统。

E.31.6 主要功能

E.31.6.1 防暴力破解

用户多次登录失败时，自动锁定登录IP。

E.31.6.2 资产管理

支持资产自动发现功能，支持手动添加资产。

E.31.6.3 漏洞库标准

漏洞库应具备CVE、CNNVD、CNVD等编号。

E.31.6.4 规则库升级

支持自动/手动/本地升级/代理服务器等升级方式。

E.31.6.5 扫描信息

包括主机信息、用户信息、服务信息、漏洞信息等内容。

E.31.6.6 扫描策略

可以并行地检查多个被评估的系统，能够提供扫描策略定制，可以保证扫描的安全性，不影响应用系统和网络业务的正常运行。

E.31.6.7 扫描功能

支持主机存活探测，支持弱口令扫描。

E.31.6.8 支持的设备类型

支持工控设备如SCADA、DCS、PLC等，以及网络设备漏洞、主机系统漏洞等，并提供安全解决建议。

E.31.6.9 工控设备支持

支持扫描西门子、施耐德、Samsung、研华、罗克韦尔、松下、罗杰康、霍尼韦尔等厂商的工控系统。

E.31.6.10 工控协议支持

支持识别主流工控协议，如S7,Modbus,IEC104,ENIP,FINS，Crimson、DNP3、Ethernet/IP等。

E.31.6.11 安全基线

支持对工控系统进行安全基线检查。

E.31.6.12 安全性检查

支持对扫描对象脆弱性检查，如安全补丁、口令、服务配置等。

E.31.6.13 威胁分级

应可对安全的威胁程度分级，形成风险趋势分析报表。

E.31.6.14 告警方式

支持扫描完成后进行SNMP trap告警、短信告警等。

E.31.6.15 报表功能

报告具有漏洞描述和安全修补方案建议，并提供相关的技术站点供管理员参考。

E.31.6.16 报告查询

支持按照任务、主机、资产等多种方式查询。

E.31.6.17 结果对比

支持同一任务的两次扫描结果对比，清晰的展示漏洞状态的变更情况。

E.32 网络数据防泄露

E.32.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.32.2 设备性能

建议根据实际业务带宽进行选型。

E.32.3 部署方式

支持单机部署，双机部署、分布式部署等。

E.32.4 工作模式

支持直路透明串接、旁路端口镜像模式。

E.32.5 系统要求

采用经过系统加固的专有操作系统。

E.32.6 性能要求

建议根据实际需要进行数据泄露检测的终端数量和应用层检测吞吐量综合考虑，并有冗余。

E.32.7 主要功能

E.32.7.1 协议识别

支持HTTP协议、TTPS协议、邮件协议（SMTP、POP3、IMAP）、FTP协议、SMB协议、NNTP协议、IM协议等的识别。

E.32.7.2 邮件识别

支持识别Webmail应用的关键信息，如发件人、收件人、主题、正文等，可支持qq邮箱、163邮箱、139邮箱、新浪邮箱等。

E.32.7.3 网盘识别

支持识别网盘上传的文件，如百度网盘、华为网盘等。

E.32.7.4 社交应用识别

支持识别社交网络的关键信息，如主题、正文、附件等，支持腾讯微博、新浪微博、QQ空间、百度贴吧等应用。

E.32.7.5 文件识别

支持识别加密文件、压缩文件、图片、文档相似度、非Windows文件、未知文件、自定义文件类型等。

E.32.7.6 内容识别

支持基于关键字、正则表达式、数据标识符、数据库指纹、文档指纹、机器学习、图片内容指纹、图片OCR等方式识别敏感内容。

E.32.7.7 异常行为识别

支持识别文档多层嵌套、文件多层压缩、文件加密、修改文件扩展名、图片格式嵌入敏感文档、拷贝文档部分内容、少量多次泄漏等方式逃避检测的行为。

E.32.7.8 响应能力

支持阻断HTTP/HTTPS/SMTP/FTP协议的响应动作，支持邮件告警、Syslog联动响应告警等方式。

E.32.7.9 策略灵活性

单条策略可以包含多个规则，内部规则之间可以通过与或非条件灵活组合。

E.32.7.10 内容策略

支持基于内容制定策略，还能结合发送者/接收者、文件特征等制定策略。

E.32.7.11 例外策略

支持针对特定数据内容，例如关键字、文件类型、文件大小、协议等条件进行例外处理。

E.32.7.12 报表方式

支持提供最近30天事件、全部事件、本周事件、按策略汇总等事件报表方式。

E.32.7.13 事件记录

系统记录事件信息包含协议类型、附件、匹配次数、发送者（邮箱，IP，用户名）、接收者（邮箱，IP，用户名）、时间、严重性等。

E.32.7.14 报表导出

事件报表支持以PDF、CSV、HTML等格式导出。

E.32.7.15 报表外发

支持定时发送、周期性以邮件方式外发等。

E.32.7.16 事件审计工作流

支持批量审计、批量下载事件附件、高亮显示违规策略、事件归档等功能。

E.32.7.17 权限管理

提供系统管理员，策略管理员，审计员等。

E.32.7.18 分级权限管理

支持实现本部门的管理员只能配置本部门的策略，查看本部门的事件报表等。

E.32.7.19 账号安全

支持用户名、口令的复杂度设定，支持空闲超时时间断开等机制。

E.32.7.20 第三方对接

系统提供SNMP接口、syslog接口、LDAP接口等与第三方系统对接。

E.33 终端数据防泄露

E.33.1 客户端资源占用

资源占用小，不影响用户日常使用。

E.33.2 系统兼容性

客户端兼容Windows XP及更高版本windows系统。

E.33.3 主要功能

E.33.3.1 客户端管控

未经授权不能对客户端卸载、关闭，不能通过任务管理器关闭客户端。

E.33.3.2 服务端安全

服务端支持用户名和口令的复杂度设定，支持超时断开。

E.33.3.3 文件识别

支持识别加密文件、压缩文件、图片、非Windows文件等。

E.33.3.4 内容识别

支持基于关键字、正则表达式、数据标识符、数据库指纹、文档指纹、机器学习、图片内容指纹、图片OCR等方式识别敏感内容。

E.33.3.5 异常行为识别

支持识别文档多层嵌套、文件多层压缩、文件加密、修改文件扩展名、图片格式嵌入敏感文档、拷贝文档部分内容、少量多次泄漏等方式逃避检测的行为。

E.33.3.6 终端监控

可基于打印、传真、CD/DVD刻录、蓝牙连接、U盘拷贝、剪切板粘贴、截屏、网站论坛、邮件、网盘上传、即时通讯工具、网络共享等方式外发敏感信息进行监控。

E.33.3.7 终端扫描

可指定包含或排除特定的文件名、文件路径、文件大小范围、文件修改时间、文件访问时间等因素进行扫描，支持通配符，可限定扫描过程中对终端的最大CPU占用率。

E.33.3.8 终端保护

可在泄漏数据时进行阻断、邮件告警、消息弹框、用户自行选择、加密数据、先阻断再审批放行、隔离敏感数据等措施。

E.33.3.9 内容策略

支持基于内容、结合发送者/接收者、文件特征等制定策略。

E.33.3.10 例外策略

支持针对特定数据内容，如关键字、文件类型、文件大小、等条件进行例外处理。

E.33.3.11 报表方式

支持提供最近30天事件、全部事件、本周事件、按策略汇总等事件报表方式。

E.33.3.12 时间记录

系统记录事件信息包含协议类型、附件、次数、发送者（邮箱，IP，用户名）、接收者（邮箱，IP，用户名）、时间、严重性等。

E.33.3.13 报表导出

事件报表支持以PDF、CSV、HTML等格式导出。

E.33.3.14 报表外发

支持定时发送、周期性邮件外发等。

E.33.3.15 事件审计工作流

支持批量审计、批量下载事件附件、高亮显示违规策略、事件归档等功能。

E.33.3.16 权限管理

提供系统管理员，策略管理员，审计员等角色。

E.33.3.17 分级权限管理

支持本部门的管理员只能配置本部门的策略，查看本部门的事件报表等，实现分级权限管理。

E.33.4 第三方对接

提供SNMP、syslog、LDAP接口等与第三方系统对接。

E.34 数据脱敏系统

E.34.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.34.2 设备性能

建议根据实际数据脱敏数度要求进行选型。

E.34.3 部署方式

支持单机部署，双机部署、分布式部署等。

E.34.4 系统要求

采用经过系统加固的专有操作系统。

E.34.5 性能要求

建议根据每小时需要脱敏的数据库容量进行选型。

E.34.6 主要功能

E.34.6.1 数据库类型

支持Oracle、SQL Server、Sybase、MySQL等数据库。

E.34.6.2 脱敏算法

支持数据假名化，数据屏蔽，数据泛化取整，数据加密，数据噪声添加，数据乱序排序等数据脱敏算法。

E.34.6.3 数据脱敏规则

支持置空、固定、乱序、姓名、身份证号、地址、电话、银行卡号、字符串屏蔽、随机、邮箱、公司名称、IP地址、URL地址、日期、加密、泛化、字典等规则。

E.34.6.4 敏感数据域

支持姓名、身份证号、手机号码、地址、公司名称、银行卡号、邮政编码、邮箱地址、IP地址、统一社会信用代码、组织机构代码、营业执照号码、URL网址、军官证号码、日期等敏感数据定义。

E.34.6.5 项目管理

支持用户创建项目、管理项目。

E.34.6.6 数据源管理

一个项目可以管理多个数据源，包括数据库、文件等。

E.34.6.7 策略支持

一个项目可包含多个策略，策略具有不同的安全级别，用于实现不同的数据脱敏目标。

E.34.6.8 任务执行

支持单次执行、周期执行、定时执行等执行方式。

E.34.6.9 任务管理

支持查看、启动、停止、暂停、继续等任务操作。

E.34.6.10 脱敏结果

支持抽查执行脱敏后的结果样例，验证脱敏是否合规。

E.34.6.11 数据库迁移

支持将数据库从源数据库迁移至目标数据库。

E.34.6.12 数据抽取方式

支持数据库到数据库、数据库到文件、文件到文件、文件到数据库、异构数据库之间的数据抽取等方式。

E.34.6.13 子集抽取

支持从原始数据库中,抽取部分数据进行脱敏。

E.34.6.14 脱敏方式

支持数据库到数据库、数据库到文件、文件到文件、文件到数据库、跨库数据脱敏、纯内存脱敏等，保持各脱敏方式下数据关联性。

E.34.6.15 权限管理

针对不同用户设置不同角色，不同角色设置不同权限，不同业务对象授权给不同用户，实现全方位的权限保护。

E.34.6.16 角色管理

支持系统管理员、安全管理员、审计管理员等角色。

E.34.6.17 审批流程

在对敏感数据进行操作，如申请数据源、数据发现、数据抽取、数据脱敏时，应提供审批流程管理，审批后才能执行数据脱敏任务。

E.34.6.18 用户管理

支持用户的创建、修改、删除等。

E.34.6.19 账号安全

支持在短时间内多次登录失败后进行账号锁定。

E.34.6.20 操作行为审计

支持脱敏审计、抽取审计、发现审计等操作审计

E.35 存储备份一体机

E.35.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.35.2 设备性能

建议根据实际备份速度、备份容量、CPU性能要求进行选型。

E.35.3 部署方式

支持单机部署，双机部署、异地灾备等。

E.35.4 系统要求

采用经过系统加固的专有操作系统。

E.35.5 主要功能

E.35.5.1 重复数据删除

设备支持重复数据删除功能，不另行收费。

E.35.5.2 数据压缩

支持分级压缩，可选择压缩级别。

E.35.5.3 SSD固态缓存

支持使用SSD固态硬盘作为数据写入缓存。

E.35.5.4 全局热备盘

支持全局热备盘功能，可定义部分硬盘为热备盘。

E.35.5.5 网卡聚合

支持网卡聚合功能，可实现网卡线路冗余。

E.35.5.6 网络环境

支持LAN备份、支持SAN结构下的LAN-FREE备份。

E.35.5.7 数据库支持

支持Oracle、Sybase、SQL Server、各种国产数据库等的联机备份及快速恢复和异机恢复。

E.35.5.8 文件备份

支持Linux, windows操作系统下的文件备份，支持快速打包备份、备份任务自动拆分功能，可针对细碎文件进行有效的备份处理。

E.35.5.9 操作系统

支持windows、Linux等操作系统备份。

E.35.5.10 虚拟机备份

支持VMware虚拟机服务器端备份。

E.35.5.11 邮件备份

支持邮件备份，支持单独恢复单一邮件。

E.35.5.12 备份方式

支持远距离备份，断点续传、脱机备份，双向缓冲、流量控制等功能，支持一对一，一对多，多对一的备份方式，支持全备份、增量备份、差分备份等多种备份方式。

E.35.5.13 介质管理

支持各种主流的磁带库产品，支持全面管理备份介质，支持对磁带库运行状况实时监控，支持D2D2T备份，实现数据磁带出库保存。

E.35.5.14 平台支持

服务端支持主流Unix平台，客户端端需支持windows、Linux、Unix系统等。

E.35.5.15 策略管理

支持备份策略的导出，支持备份策略的共享。

E.35.5.16 备份管理

支持对已备份文件进行检索查询，支持一次性恢复多次备份任务下多个文件。

E.35.5.17 用户权限

支持不同级别的用户权限控制。

E.35.5.18 快速恢复

支持当在线数据或操作系统故障时，备份系统快速从备份设备中恢复最新时间点数据或操作系统。

E.36 态势感知系统

E.36.1 基本要求

拥有自主知识产权。

E.36.2 操作系统

支持跨平台部署，支持运行于Windows或Linux。

E.36.3 软件架构

基于B/S架构，全中文界面。

E.36.4 部署方式

支持私有化部署或云端部署，支持SaaS多租户模式。

E.36.5 扩展性

具有开放的接口体系，能够与第三方系统对接。

E.36.6 主要功能

E.36.6.1 风险态势

支持对各类安全对象进行多维度监控，从安全事件、脆弱性、部门、业务、操作系统等维度呈现风险分布情况。

E.36.6.2 态势展示

支持风险指数、资产信息、、攻击方式排名等态势展示。

E.36.6.3 威胁态势

支持基于事件类别、攻击来源、攻击手段、攻击时间、攻击IP、次数、端口等进行图形化展示和统计。

E.36.6.4 安全底图

从管理视角展示全网的防护设备保障能力、人员安全保障能力，从运维视角展示详细资产信息、安全人员数量、防护设备详情等。

E.36.6.5 资产信息底图

立体化呈现资产信息、服务器信息、业务系统信息、脆弱性指数等，多维度展示网络安全情况。

E.36.6.6 安全处置态势

支持对安全事件告警的处置管理，提供告警级别分布、告警趋势等展示模块，对已处置告警、未处置告警进行实时展示。

E.36.6.7 资产态势

支持展示资产总量、脆弱性总数、资产相关联的攻击事件等，支持从安全事件影响范围、发起攻击的资产等多个粒度进行分析。

E.36.6.8 脆弱性态势

描述整体网络脆弱性，包括脆弱性所关联的资产、漏洞类型和漏洞级别的变化趋势、高危漏洞TOP10等，对漏洞全生命周期进行跟踪，详细展示漏洞影响范围，影响的资产、关联漏洞的编号及漏洞详情等。

E.36.6.9 攻击态势

从实时攻击视角出发描述网络安全整体情况，地图呈现实时动态攻击行为和攻击属性，包括事件名称、类型、级别、发生时间等。

E.36.6.10 自定义态势

支持基于不同时间对安全态势进行展示定义，展示方式如表格、树型图、指示灯、2D图表(饼图、柱图、曲线图等)、3D图表(饼图、柱图、曲线图等)、雷达图、热度图、地图、幻灯片等。

E.36.6.11 脆弱性检测

支持脆弱性收集、脆弱性维护、扫描器管理等。

E.36.6.12 脆弱性管理

脆弱性维护管理模块可展示资产的脆弱性信息以及变更历史，支持对结果进行对比分析，可在本模块进行漏洞的全生命周期管理。

E.36.6.13 第三方接口

提供第三方脆弱性收集接口，支持外部扫描报告导入。

E.36.6.14 扫描器管理

扫描器管理模块实现对扫描器状态、任务的统一管理，用户可进行扫描任务创建、控制、下发等操作；在任务扫描完成后，可在系统上查询扫描结果。

E.36.6.15 扫描器支持

支持多种类型的扫描器，包括系统漏洞扫描、Web漏洞扫描、配置核查、数据库扫描等，支持主流漏洞扫描厂商。

E.36.6.16 安全事件管理

支持对安全事件按照优先级、事件类型、设备类型等进行管理。

E.36.6.17 安全事件检索

支持对安全事件的检索，支持基于地址、类型、端口、时间等信息进行检索。

E.36.6.18 安全状况监测

支持获取每条事件的详细记录、查看相关安全对象信息、派发工单处理事件，从而掌握整体网络运行状况。

E.36.6.19 安全事件溯源

可针对安全事件进行一键溯源，根据IP五元组、设备类型、资产责任人等信息展示攻击路径。

E.36.6.20 攻击关联分析

支持以攻击状态机方式对海量数据进行关联分析，根据分析结果发现和预测攻击事件。

E.36.6.21 告警管理

支持对安全告警的全面管理，如可批量确认、消除告警，展示告警详情，确认、追溯、清除及关联安全经验库进行处置等。

E.36.6.22 告警创建

支持预警的自动发布和手工创建，预警信息包括预警名称、类型、预警级别、内容、可能后果等。

E.36.6.23 工作台

提供处置工作台，用户可进行工单创建、工单派发、工单监控、工单归档等操作。

E.36.6.24 工单状态

支持图形化的方式展示工单当前状态。

E.36.6.25 工单归档

支持对已完成工单的工单归档功能。

E.36.6.26 报表格式

内置多种报表模板，支持word、pdf、excel等格式。

E.36.6.27 报表任务下发

支持设置下发报表任务，支持手动、自动下发方式。

E.36.6.28 资产风险评估

支持基于资产的价值、安全脆弱性、安全威胁等因素进行关联分析，评估资产风险。

E.36.6.29 风险计算

提供针对安全域内资产的风险计算，统计分析安全域的风险情况。

E.36.6.30 资产维护

支持对资产的维护，基于IP、型号、版本等特征，实现对资产的增删改查。

E.36.6.31 资产探测

支持全网资产的自动探测。

E.36.6.32 威胁情报数据

支持对接各类威胁情报数据，如恶意IP库、恶意样本信息、钓鱼网站、垃圾邮件、全球被黑网站等。

E.36.6.33 威胁情报管理

支持对各类威胁情报数据进行增删该查、属性修改、导入导出等。

E.36.6.34 黑白名单

支持通过内置的黑白名单机制对恶意威胁信息进行标记，阻止等。

E.36.6.35 安全事件追踪溯源

针对安全事件进行追溯，对攻击对手、攻击方式、攻击路径、攻击源、攻击目标、攻击后果进行拓展分析，通过数据融合、数据关联重新刻画安全事件。

E.36.6.36 IP画像

利用先进的IP画像技术，从物理和逻辑两个维度将相应IP的属性信息进行关联及标签化处理；通过对单一IP的具象描述，能够在安全事件发生后，快速定位受影响资产，提高安全响应能力。

E.36.6.37 安全知识库

提供各类安全知识库，如漏洞库、补丁库、病毒库等。

E.36.6.38 标准规范管理

支持对国家、行业、企业要求的相关文档或规范的集中存储管理，支持文件共享和分发等；支持对文档增、删、改、查及属性的编辑。

E.36.6.39 应急预案库

内置多场景应急预案库，如设备故障、网络攻击、信息破坏等场景，对应急工作提供决策支撑。

E.36.6.40 用户管理

基于角色认证模式，提供系统用户、系统操作员、审计员等角色。

E.36.6.41 告警

支持多种告警与响应方式，提供灵活规则定义能力。

E.36.6.42 过滤器

支持多种过滤器，快速过滤无关信息。

E.36.6.43 风险参数管理

依据ISO/IEC 27000安全标准，多维度计算安全对象所面临的风险数值，参数包括资产属性、脆弱性漏洞、安全事件等。

E.36.6.44 日志审计

支持自身日志审计，包括管理日志、服务器、安全设备等日志的导出。

E.36.6.45 日志收集方式

支持主动/被动日志数据收集。

E.36.6.46 日志解析

日志解析包含接收时间、事件类型、事件名称、报警级别、IP、设备类型等属性。

E.37 运维堡垒机

E.37.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.37.2 设备性能

建议根据实际需要运维的网络设备点数进行选型。

E.37.3 部署方式

支持旁路部署。

E.37.4 系统要求

采用经过系统加固的专有操作系统。

E.37.5 主要功能

E.37.5.1 用户管理

支持账号的创建、维护、修改、删除等。

E.37.5.2 临时用户

针对临时用户建立有效期，过期自动注销。

E.37.5.3 访问策略

支持指定密码有效期和密码强度，支持指定密码错误次数和锁定时间，支持在指定时间内访问相关资源。

E.37.5.4 资源统计

支持查看系统中不同资源所占总资源比例。

E.37.5.5 资源类型

支持Unix资源、网络设备、windows资源、数据库资源、C/S资源、B/S资源、中间件资源等。

E.37.5.6 资源协议

支持SSH、TELNET、FTP、VNC、XWINDOW文件共享等协议。

E.37.5.7 自动改密

支持对资源密码变更，支持根据密码策略要求进行变更。

E.37.5.8 密码拨测

定期检查平台存储的设备账号密码与实际密码是否匹配。

E.37.5.9 动作流代填

将单条动作转换为一系列操作代替人工输入。

E.37.5.10 账号导出

支持账号导入导出，支持账号导出的密码验证。

E.37.5.11 角色管理

角色权限细粒度高，可自由组合，实现分层分级管理。

E.37.5.12 岗位授权

资源授权模式基于岗位，岗位上绑定资源账号。

E.37.5.13 收藏夹

支持将经常访问的资源添加到收藏夹。

E.37.5.14 批量单点登录

支持一键批量登录选中的资源。

E.37.5.15 身份认证

支持自身认证，同时支持与第三方认证结合。

E.37.5.16 访问时间策略

支持限制在指定时间可访问/不可访问相关资源。

E.37.5.17 地址策略

支持访问源IP地址的限制。

E.37.5.18 字符命令

支持命令操作的黑白名单，可以对命令的参数进行限制。

E.37.5.19 脚本自动化执行

支持网络设备的脚本自动化执行。

E.37.5.20 远程桌面审计

支持对RDP实时会话的锁定和解锁。

E.37.5.21 RDP审计

支持审计录像的画质选择，支持多种画质。

E.37.5.22 字符审计

对字符命令方式的访问可以审计到所有交互内容，支持高亮显示高危命令。

E.37.5.23 实时监控

支持实时审计和阻断，发现高危操作时，支持实时切断。

E.37.5.24 管理审计

支持系统内部操作审计。

E.37.5.25 审计报表

支持以syslog形式分类外发。

E.37.5.26 审计分权

不同权限的人员，按照所属组查看授权的审计信息。

E.37.5.27 审计报表

提供基础业务报表、行为审计报表、信息管理报表等，支持Word、Excel、PDF等类型下载，支持周期性生成，自动外发至指定邮箱。

E.37.5.28 登录审批

支持将指定资源设置登录审批，审批通过后才可登录。

E.37.5.29 命令审批

支持将高危命令设置为执行需审批策略，当指定资源执行高危命令时，需要审批通过后，命令才能执行生效。

E.37.5.30 消息管理

支持管理员发布公告，通知运维用户，公告在指定时间可以看到，过期自动删除。

E.37.5.31 系统状态

支持监测CPU、内存、磁盘、网卡等的工作情况。

E.37.5.32 外接存储

支持日志数据的外置存储备份。

E.37.5.33 可靠性技术

支持双机热备和双网卡链路聚合技术。

E.37.5.34 会话保持

支持RDP图形协议在双机部署下的会话保持功能。

E.38 网站安全监控系统

E.38.1 物理接口要求

千兆电口，千兆/万兆光口等按需选择。

E.38.2 设备性能

建议根据实际需要并行监控的网站数量进行选型。

E.38.3 部署方式

支持旁路部署。

E.38.4 系统要求

采用经过系统加固的专有操作系统。

E.38.5 主要功能

E.38.5.1 代理扫描

支持通过代理服务器的方式对网站进行统一监控。

E.38.5.2 WEB检测

支持对Oracle、MySQL、SQL Server等数据库的漏洞扫描，支持对XSS跨站脚本攻击进行扫描，支持对网络爬虫、扫描器的攻击进行扫描，支持对上传文件进行扫描，支持自定义白名单，排除已知链接，支持对Web漏洞扫描进行日志记录，记录IP地址、漏洞描述、漏洞名称等。

E.38.5.3 钓鱼检测

支持多种搜索引擎的钓鱼检测，支持保留证据。

E.38.5.4 可用性检测

支持网站的HTTP、DNS、PING响应，提供网站诊断。

E.38.5.5 木马检测

提供静态匹配和动态沙箱技术，支持保留证据。

E.38.5.6 敏感信息检测

支持网站敏感信息检测，能自定义导入敏感信息。

E.38.5.7 Web Shell

支持本地进行web shell后门的检测。

E.38.5.8 弱口令检测

提供多种弱口令检测，支持telnet、ssh、ftp等协议。

E.38.5.9 篡改监控

支持对网站发生的改动行为进行监控。

E.38.5.10 报表功能

支持以Excel、word、HTML、PDF等格式输出。

E.38.5.11 告警功能

支持首页滚动式报警，支持短信、邮件等告警方式。

E.38.5.12 日志审计

支持对系统内部操作进行审计日志记录，支持日志外发。

E.38.5.13 权限管理

支持监测引擎和管理员绑定，特定监测引擎只能被授权的管理员使用。

E.39 终端杀毒

E.39.1 B/S管理架构

管理端支持纯B/S架构，无需安装客户端软件。

E.39.2 轻量级客户端

客户端资源占用小于50MB，有效节省终端资源使用率。

E.39.3 操作系统支持

支持Windows XP、Windows 7、Windows 8、Windows 10等操作系统，支持Windows2003、Windows2008、Windows2012等服务器操作系统。

E.39.4 主要功能

E.39.4.1 可视化展示

支持全网威胁统计分析，管理控制台展示病毒趋势统计、终端信息、病毒类型排行、病毒排行等。

E.39.4.2 终端管理

管理控制台支持实时显示客户端的状态，支持对防病毒客户端进行分组，支持对全网进行集中的管理和任务下发，支持下发漏洞监测策略，支持客户端自动升级，支持基线检查等。

E.39.4.3 权限控制

支持客户端防删功能，防止客户端强行卸载；支持分级管理及多管理员权限划分，如：超级管理员，操作管理员等。

E.39.4.4 行为审计

管理控制台支持对客户端的系统操作行为进行记录。

E.39.4.5 统计分析

支持客户端威胁日志信息上报。

E.39.4.6 报表功能

报表内容包括病毒类型分析、病毒排行、终端杀毒排行等；支持将报表以Excel、word、HTML、PDF等格式输出

E.39.4.7 策略管理

控制台支持恶意网站拦截、浏览器保护、文件保护、下载保护、系统加固、U盘防护、邮件监控等；支持设置定时杀毒策略以及错峰扫描策略。

E.39.4.8 病毒查杀

支持对终端电脑进行全盘扫描、快速扫描，自定义扫描等；并支持空闲查杀、断点查杀、后台查杀等。

E.39.4.9 插件查杀

支持扫描和清除各种广告软件、恶意插件、隐蔽软件、黑客工具、风险程序等。

E.39.4.10 宏病毒查杀

支持Office/IE/Lotus Notes等嵌入杀毒。

E.39.4.11 病毒隔离

支持病毒自动隔离功能。

E.39.4.12 APT防范

支持未知病毒、恶意代码的防范能力，支持基于行为的检测和防护。

E.39.4.13 注册表查杀

支持注册表病毒、内存或服务类病毒的查杀，提高终端安全等级。

E.39.4.14 目录白名单

支持病毒查杀时目录排出功能。

E.39.4.15 云查杀

支持将未知文件上报，通过云引擎进行分析判断。

E.39.4.16 安全检测

支持U盘扫描检查功能；支持对网页进行病毒、木马进行监测及防护；支持客户端对外攻击检测，支持系统漏洞扫描功能。

E.39.4.17 实时监控

能够实时清除来自各种途径的病毒、木马、恶意程序。

E.39.4.18 邮件监控

支持对终端文件、邮件、网页一体化监控，防止病毒运行。

E.39.4.19 威胁情报

支持可疑文件上报功能，并将情报全网共享。

E.40 终端安全管理系统

E.40.1 兼容性

客户端支持windows XP、win7/8/8.1操作系统。

E.40.2 主要功能

E.40.2.1 资产管理

提供资产创建、领用、调拨、借出等全生命周期管理。

E.40.2.2 系统信息审计

可查看各主机端口、进程、服务、敏感信息、文件流转等信息。

E.40.2.3 补丁管理

提供终端补丁检测时间、下载的补丁类型、补丁级别和补丁分发。

E.40.2.4 软件分发

可指定下发时间、分发后的处理方式。

E.40.2.5 文件监控

对终端文档进行关键字检查，对含有关键字的文档进行发送、拷贝等。

E.40.2.6 设备监控

可对主机的以下设备进行启用禁用操作：如光驱、打印机、网络适配器、蓝牙设备、USB设备等，同时支持例外处理。

E.40.2.7 移动介质管理

支持对移动存储设备标签式管理，区分内外部介质。

E.40.2.8 非法外联监控

支持http、telnet、ping等检测主机违规外联行为，可设定检测周期、检测地址、违规处理方式等。

E.40.2.9 终端性能监视

可监视内存、CPU、系统盘、网卡接收发送速率、累计运行时间等，超阈值报警。

E.40.2.10 系统配置监控

支持主机系统进程、注册表、服务监控，采取黑白名单方式对用户具体操作项进行控制并审计。

E.40.2.11 主机防火墙

支持定义终端进程，指定规则名称、进程名称、协议等。

E.41 基线管理系统

E.41.1 系统管理模式

支持通过web方式管理，支持SSL加密模式传输，具备跨平台性、开放性和扩展性； 支持Android等移动终端快速执行扫描任务，浏览扫描结果等。

E.41.2 系统部署

支持独立部署、分布式部署，无需在被检系统上安装软件。

E.41.3 系统性能

单个任务允许扫描的最大扫描范围不小于一个C类IP地址；对被检查设备性能影响不超过 5%；检查结果的误报率低于 10%。

E.41.4 支持检查类型

E.41.4.1 操作系统

支持 Windows系列、Linux系列、Solaris、 HP-UX、 Centos 、Red hat、SUSE、Ubuntu、Debian、AIX 等操作系统。

E.41.4.2 网络设备

Cisco、华为、H3C、中兴、锐捷等主流网络设备。

E.41.4.3 工控设备

支持西门子、施耐德等厂商上位机的配置检查。

E.41.4.4 安全设备

支持天融信、CISCO、华为、山石网科、Checkpoint等。

E.41.4.5 中间件

支持 Apache、WebLogic、TOMCAT等。

E.41.4.6 数据库

支持 Oracle、MySQL、Sybase、DB2、SQL Server等数据库。

E.41.4.7 虚拟化设备

支持VMware ESXi等虚拟化平台。

E.41.5 脆弱性扫描与管理系统

脆弱性扫描与管理系统需要有以下功能：

a) 支持按照业务系统类型、组织结构等创建在线、离线扫描任务；支持实时、定时、周期性任务；
b) 支持历史扫描结果同屏对比，对比节点可选择；
c) 支持在线实时查看扫描进度及扫描详细情况；
d) 支持离线核查脚本下载并自动执行，离线脚本载体不限；
e) 支持对指定设备进行直接扫描，无需建立任务，生成扫描报告；
f) 支持自动发现已添加设备的版本、型号等信息；
g) 支持任务断点续扫功能；
h) 支持按照任务、设备导出扫描结果，支持 HTML、PDF、邮件等方式。

E.41.6 系统管理

支持管理员、操作员、审计员三权分离。

E.41.7 日志审计

能够对登录日志、操作日志等信息进行记录和查询，支持日志导出。

E.41.8 报表管理

内置多维度报表模板，支持通过邮件发送报表。

E.41.9 系统扩展性

支持扩展系统漏洞扫描和Web漏洞扫描功能。

E.42 网络管理系统

E.42.1 基本要求

拥有自主知识产权。

E.42.2 操作系统

支持跨平台部署，支持运行于Windows或Linux。

E.42.3 软件架构

基于B/S架构，全中文界面。

E.42.4 监控架构

支持监控扩展；支持分布式管理，能够满足大规模网络监控要求。

E.42.5 扩展性

具有开放的接口体系，能够与第三方系统对接。

E.42.6 主要功能

E.42.6.1 网络设备监控

支持各类网络设备、无线设备、安全设备的监控，能够监控设备的可用性和主要性能指标。

E.42.6.2 链路监控

支持对网络链路的监控，能够监控链路的通断和主要性能指标。

E.42.6.3 主机监控

支持各类主机系统的监控；能够监控主机系统的可用性以及主要性能指标。

E.42.6.4 数据库监控

支持各类数据库的监控，能够监控数据库的可用性和主要性能指标。

E.42.6.5 中间件监控

支持各类中间件的监控，能够监控中间件可用性和主要性能指标。

E.42.6.6 存储监控

支持各类存储阵列的监控；能够监控存储设备的可用性和主要性能指标。

E.42.6.7 虚拟化监控

支持各类常见虚拟化的监控，能够监控主要性能指标。

E.42.6.8 拓扑管理

支持网络拓扑自动发现；支持全局拓扑和子拓扑，拓扑实时展现网络设备、网络链路状态的变化，以颜色变化直观展现设备的性能变化。

E.42.6.9 策略管理

统一管理并下发监控策略并支持监控策略的自定义配置。

E.42.6.10 告警管理

支持告警策略的规则配置；可对告警进行确认、关闭、删除操作；支持声音、短信息、微信和邮件等多种告警通知方式；支持组合条件查询。

E.42.6.11 统计报表

通过内置报表和自定义报表，能够从多维度进行监控数据的统计分析；支持多种图表展现形式；支持报表导出和报表订阅。

E.42.6.12 其他

支持业务管理视图、自定义监控展现、自定义扩展监控等功能。

E.43 运维管理系统

E.43.1 基本要求

拥有自主知识产权。

E.43.2 操作系统

支持跨平台部署，支持运行于Windows或Linux。

E.43.3 软件架构

基于B/S架构，全中文界面。

E.43.4 扩展性

具有开放的接口体系，能够与第三方系统对接。

E.43.5 主要功能

E.43.5.1 资产库

管理所有配置项及其关系，以及与这些配置项有关的工单等关联信息；对配置项的全生命周期进行管控，以及资产二维码标签打印及二维码扫描追溯。

E.43.5.2 库存管理

对配置项、配件等资产的采购、入库、出库等进行管控。

E.43.5.3 服务台

服务台能快速响应各种事件，记录事件的内容，对事件进行分类，确定优先级，并派发给相应人员进行处理。

E.43.5.4 事件管理

支持故障的记录、分类、处理和解决的流程管理；支持多种报障方式，包括电话、服务台、PC、APP、Web、微信等，支持一键快速报障；工单结束后报障人可进行服务评价；支持流程跟踪、催办、移动办公等共性。

E.43.5.5 服务请求管理

支持服务请求的记录、分类和处理，确保服务尽快交付支持服务请求受理、处理、退回、升级、提交和评价的基本流程，支持协同处理，并满足相关角色间的顺畅流转。

E.43.5.6 问题管理

支持问题的记录、识别、调查、诊断和解决的流程管理；涵盖问题发起、评估及定级、分派、定位、实施解决方案、解决效果确认等基本环节；支持流程跟踪、催办、移动办公等共性。

E.43.5.7 变更管理

支持变更的请求、评估、审核、实施、确认的流程管理；包括变更请求、评估、授权、定级、计划、测试、实施、记录和评审，以及变更计划的执行和回滚等基本环节；支持流程跟踪、催办、移动办公等共性。

E.43.5.8 作业计划管理

支持灵活创建作业计划、自动分派和管理任务，生成工单以及任务提醒。通过按天、按周、按月以及一次性等周期规律来设定任务的执行时间。

E.43.5.9 服务级别管理

可以根据服务级别协议（SLA）的内容，约束对象或者流程的运营情况，触发相应控制操作并将结果呈现给用户，对待办的流程工单做时间提醒或者自动结束待办，推动流程。

E.43.5.10 流程定义

自定义流程功能的流程引擎组件。通过Web界面对工作流程的操作按钮、执行人员、执行环节进行设置，配置最适合的操作流程。

E.43.5.11 知识库

知识管理流程，包括知识的提交、审批、发布；支持知识分类、创建、审核、修改等操作，不同类别的知识支持阅读权限控制；支持知识库与工单的关联；提供关键字、全文检索等检索方式；支持知识评价打分。

E.43.5.12 态势感知

以资产、人员、事件等要素为基础，采集并清洗需要的数据，分析得出各个重要指标可视化的呈现给用户，使用户能够直观的掌握运维全局状况。

E.43.5.13 运维统计分析

通过多维度、多视角对运维数据的分析统计，生成不同统计报表及图形报表。

E.43.5.14 运维机器人

运用智能检索及算法对知识及工单进行运算，快速解答运维人员提出的问题，能够提供故障解决方案的智能推荐以及工单的智能派发。

E.43.5.15 值班管理

电子化值班管理，包括排班配置、排班管理、替换班管理、值班日志管理和交接班等功能。

E.43.5.16 项目管理

实现对项目全生命周期的管控，同时将项目过程与工单紧密结合，形成项目信息化闭环。

E.43.5.17 手机APP

能够让运维人员通过移动端APP操作运维管理软件相关功能，APP支持安卓和IOS。

E.43.5.18 其他

支持微信小程序、客户管理、协同办公等功能。

E.44 日志审计系统

E.44.1 基本要求

拥有自主知识产权。

E.44.2 操作系统

应支持跨平台部署，支持运行于Windows或Linux。

E.44.3 软件架构

基于B/S架构，全中文界面。

E.44.4 主要功能

E.44.4.1 日志采集

支持通过多种方式，对设备日志、应用日志、访问链路过程以及业务日志进行全面采集。

E.44.4.2 日志结构化

提供多种方式对非结构化的文本日志内容进行结构化，并且通过一系列规则和算法机制完成对结构化后的数据的预处理工作。

E.44.4.3 日志检索

采用全文检索技术对收集的各类型日志进行检索定位，提供基于关键词、自定义规则等检索方式。支持将检索结果以多种图表方式进行统计展示。

E.44.4.4 自助式分析

提供基于B/S的在线可视化日志图表设计器，可以灵活的组合各类型的日志数据进行统计分析展现。

E.44.4.5 分布式跟踪分析

能够跟踪业务访问过程的业务模块访问情况和链路访问情况，为业务各环节的性能分析、故障定位溯源、应用容量管理规划提供可靠依据。

E.44.4.6 业务健康指数评估

通过算法对业务应用域的运行健康状况进行数值化评估，能够直观的了解业务运行的健康状况。

E.44.4.7 容量管理与评估

结合业务、服务和资源容量的需求，对容量进行评估、规划、分析、调整和优化，以保证对资源的最优利用。

E.44.4.8 场景式专题分析

提供一些场景式专题分析模板和技术分析专题模板，能够快速满足常见的分析需要。

参 考 文 献

[1] 国卫规划发〔2018〕23号　国家健康医疗大数据标准、安全和服务管理办法（试行）
[2] 国卫规划发〔2017〕6号 “十三五”全国人口健康信息化发展规划》的通知
[3] 粤卫办函〔2012〕2号　全面开展全省卫生行业信息安全等级保护工作
[4] 卫办发〔2011〕85号　卫生行业信息安全等级保护工作的指导意见
[5] XXX 基于电子病历的医院信息平台建设技术解决方案（1.0 版）技术部分
[6] XXX 国家医疗健康信息医院信息互联互通标准化成熟度（医院信息互联互通）测评方案