3医联体协作、数据汇聚、共享管理平台

3.1信息前置管理平台

信息前置管理平台是XX新区医院数据中心进行数据共享的中转站， 定期采集或导入运营数据及科研数据， 用于规范数据的存储结构， 并采用技术手段对纳入的数据进行严格的审查与清洗，以便于后期数据的使用与共享。

3.1.1大数据采集

采集中心子系统主要向采集前置机派发采集任务， 采集前置机执行采集任务并将采集数据文件传输至采集中心， 采集中心收到数据文件后通知大数据中心进行入库； 采集中心子系统需要对各被采集的医疗机构管理、元数据管理、采集管理、采集报表、调度管理及实现前置机远程升级。

为保障数据采集的稳定有序运行， 采集中心将会分发采集任务至各家机构的采集前置机， 采集前置机负责执行采集任务， 针对不同类型的任务， 前置机通过 不同的服务来执行。

3.1.1.1机构管理

- 可对接入采集中心的机构信息如机构名称、机构编码、经营性质等进行管 理，包括增加、修改和删除等；
- 可对机构的基本信息进行查询和检索；
- 当遇到特殊情况需要临时暂停改机构采集任务时， 可关闭指定机构的采集任务，同时在有需要时可重新开启采集任务。

3.1.1.2元数据管理

- 可对接入采集中心的医疗机构各业务系统的数据表进行管理， 包括数据表类型、表重要性、表见关系等；

➢可对医疗机构的元数据日志进行管理，包括业务系统元数据的变化情况，如增加、修改、删除了那些表或字段等。

3.1.1.3采集管理

➢为满足科研、人工智能等批量数据应用需求，可支持获取增量数据的接口，通过管控列标识来实现增量数据的采集方式；

➢根据采集前置机和接入结构负载能力的不同，可制定不同的采集策略，以降低数据采集对源系统的影响；

➢可按照采集规则生成采集任务，通过调度程序发送至采集前置机由其执行采集任务；

➢可保障采集前置机的稳定运行，包括监控前置机的状态、运行服务组件，

实现智能化运维；

➢可在数据采集过程中对医疗机构数据库中存在的、与大数据中心存储引擎有差异的特数字符进行转换后进行存储。

3.1.1.4质量管理

➢支持通过报表方式分析数据采集的完整性，分别从数据汇总、任务汇总、明细三个为分析；

➢支持在特定时间内采集的数据和机构源数据进行数据量对比，确保数据采集符合预期，保障数据采集的完整性。

3.1.1.5调度管理

➢支持采集规则定时启动采集任务或关闭采集任务；

➢支持根据各节点任务饱和度实时派发任务；

➢支持根据网络流量负载实时调整传输任务；

➢在特定时间内采集的数据和机构源数据进行数据量对比，确保数据采集符合预期，保障数据采集的完整性。

3.1.1.6远程升级

支持采集系统的远程升级， 同时在测试发生问题时可在线回滚， 确保远程升级可靠性。

3.1.1.7数据采集服务

支持对采集中心派发结构化数据的采集任务， 实现对医疗机构结构化数据的采集并回传至采集中心， 采集任务信息包括数据文件输出路径、数据文件名、字段分隔符、脚本执行状态等。

3.1.1.8影像采集服务

支持对采集中心派发影像数据的采集任务， 对医疗机构的影像文件进行采集，并将所采集的影像文件按照任务要求回传至采集中心。

3.1.1.9数据加密

为增加数据传输过程中的安全性， 采集任务将采集数据文件传输至采集中心过程中， 采集数据除了通过选用 AES，RSA，MD5 等加密方式外， 在每个任务的数据文件中加入不同随机的混淆字符进行加密，增加额外的安全性。

3.1.2大数据管理

大数据管理是整个健康医疗大数据平台的功能枢纽， 需存储大数据采集完成的数据， 实现对数据的统一存储管理； 需接收大数据治理的数据治理逻辑并将其转化为可执行作业， 通过这些作业的执行真正实现数据治理过程； 需响应来自大数据检索和大数据服务的请求，提供数据查询检索和数据抽取服务。

3.1.2.1作业管理

- 支持对作业分类管理，用户可自行创建和维护作业类目录树；
- 支持作业的配置管理，提供作业创建、修改、删除和查询功能
；
- 支持作业的调度策略配置管理， 提供调度策略的创建、修改、删除和查询功能；

➢支持对一个作业的若干任务的配置， 提供任务的创建、修改、删除和查询功能；

➢任务调度引擎可实现对任务和作业的状态维护， 包括对作业的提交、对已提交任务的执行状态跟踪以及执行错误任务的处理等；

➢支持对作业执行状态以及任务执行结果的监控；

➢支持通过可视化界面编辑 SQL 和相关配置完成 ETL 流程；

➢任务调度引擎支持定时时间触发执行数据处理任务；

➢任务调度引擎支持数据从医院采集到大数据入库再到中间层、集市层的完整依赖链。中间层依赖的相关医院表的所有采集任务完成后执行相关数据处理、 转换任务。

3.1.2.2数据计算管理

➢支持流失数据处理引擎和批量数据处理引擎；

➢支持对数据计算任务分配的资源管理，包括CPU、内存、磁盘和网络等；

➢支持对数据计算任务的执行情况进行监控并将结果反馈至其他监控运维 系统。

3.1.2.3数据存储管理

➢可提供多种查询接口及定时任务，虚拟表到物理表之间的映射管理服务；

➢可根据不同的数据使用场景和数据存储性能要求， 提供不同的存储引擎支持；

➢可提供标准 SQL 语法查询、统一元数据服务、统一权限控制服务等查询检索功能；

➢可根据业务需求将数据划分为贴源层数据、标注层数据等，并进行管理。

3.1.2.4多租户管理

支持对用户接口、服务接口和权限中心的分别管理。

3.1.2.5运维监控

➢可为运维人员提供图形化的管理平台；

➢运维人员可通过图形化界面对主机进行管理， 包括主机增加、维护、删除等;

➢运维人员可在运维管理系统对服务组件启停、迁移、维护和删除；

➢可通过运维监控系统实现自动化系统部署和服务升级服务；

➢对已可视化图标方式展示运维监控的各项指标， 并对关键指标进行监控告警。

3.1.2.6跨异构数据库混算

提供统一的虚拟数据库， 支持虚拟表到物理表之间的映射， 终端用户无需关心数据的物理存放位置和底层数据源的特性即可操作数据， 体验类似操作一个数据库。用户只需通过统一 SQL 语言，即可透明实现跨异构数据系统混算和写出。

3.1.3大数据治理

大数据治理将为健康医疗大数据提供数据标识、数据统一规范、数据转换、 流程监控、质量监控以及数据清洗和生命周期等业务支持、为大数据应用与服务 提供数据分析策略。

3.1.3.1数据标准管理

➢可提供符合业务需求和行业共识的数据标准定义， 并可对数据标准进行维 护;

➢可提供数据字典描述、数据字典值域统一及数据字典值域描述标准化服务， 实现对国家标准、行业标准、低于标准等字典的统一存储；

➢可对敏感数据字段进行脱敏处理，脱敏方式支持在线脱敏和离线脱敏；

➢可支持多家机构的数据做字典标准化映射；

➢可支持从大数据数据库定时获取待做标准化的数据；

➢提供标准化映射模板，实现批量标准化字典映射。

3.1.3.2数据标识管理

➢可对各医疗机构数据结构和关系进行标识，建设映射关系

； ➢可对各业务表字典之间的关联关系进行管理；

➢可对各医疗机构原始数字字典进行管理；

➢可保证在数据脱敏后保持原有数据特征、业务规则和数据关联等， 保障脱 敏对后续业务无影响。

3.1.3.3元数据管理

➢可对不同医疗机构信息化厂家的系统、表字典、表字段等信息进行管理；

➢可对不同医疗机构元数据采集提供数据库信息采集配置、数表字典信息采 集配置和数据表字段信息采集配置等；

➢可对不断更新的医疗机构的元数据进行校验；

➢可实现医疗机构元数据离线采集和在线采集；

➢可通过元数据检索实现对医疗机构、系统厂家、数据表、字段等信息的查 询。

3.1.3.4主数据管理

➢可对健康医疗大数据平台的主数据， 包括数据集、元数据表及元模型进行管理；

➢可实现对主数据进行查询、修改、审核、发布等功能。

3.1.3.5数据建模管理

可根据数据需求模型， 监理不同的数据服务集市， 并可对数据建模后的数据结构进行新增、修改和删除，以及表和字段信息的设计和创建功能。

3.1.3.6血缘关系分析

➢可实现不同数据节点的数据血缘关系的汇聚和管理；

➢可以图形化的方式展现不同数据的血缘关系。

3.1.3.7数据质量监控

➢可灵活定义数据质量控制的维度， 包括数据完整性、规范性、一致性、准确性等;

➢可对数据质量控制的流程进行配置和修改;

➢可定期生成数据质量检测报告，并提供给管理人员进行查询。

3.1.3.8数据转换规则管理

➢可对数据转换任务进行定义和管理， 包括任务版本、任务调度信息、任务定义及任务状态等;

➢可实现原始医疗机构数据到标准仓库的数据转换配置。

3.1.3.9数据治理成果

➢基于国家及行业规范， 健康医疗大数据平台应提供不低于 10个业务主题、200 个以上临床数据集、 400 个以上数据字段及 8000 个以上元数据规范;

➢可实现国家健康医疗大数据中心(XX)所汇聚的 37 家二级及以上医疗机构的数据的的治理工作，并实现与XX医院业务数据中心的互联互通。

3.1.4大数据查询检索

大数据查询检索是解决各家医疗机构的不同存储类型的数据不断汇聚而产 生的海量数据的高效交互式查询问题， 为医疗数据的使用提供一个稳定可靠的查 询能力。

随着各家医疗机构的数据汇聚， 健康医疗大数据平台的数据量将迅速膨胀，预计达到 TB 甚至 PB 级别。在数据的使用分析过程中， 要求能高效对数据进行处 理； 通过使用大数据查询引擎来检索数据， 解决查询效率低下问题， 存储引擎和 查询引擎的选型需要综合考虑存储效率和查询效率问题， 让存储和查询能够更好 地起到协同作用。

3.1.4.1资源目录

对数据资源可实现数据库维度和业务分类维度两种不同的管理和查看方式。

3.1.4.2交互式查询

➢用户可自定义查询条件对数据进行检索和查询；

➢可提供标准 SQL 语法的查询工具。

3.1.4.3患者视图

可全面展示患者健康医疗大数据的相关信息， 包括基本信息、就诊记录、检查信息、检验信息、处方信息等。

3.1.4.4数据交互设计

➢支持以微服务方式对内对外提供 API 接口服务；

➢可提供数据源目录接口、数据源查询接口、交互查询接口、数据表信息接 口、数据表列表接口等。

3.1.4.5跨语言接口调用

支持可扩展且跨语言的服务开发， 能让不同的编程语言调用大数据查询检索平台的接口。

3.1.4.6跨存储引擎查询

由于存储系统支持不同的存储引擎， 查询检索平台应支持不同的存储引擎的查询，实现跨异构数据库混合查询。

3.1.5患者主索引

通过建立主索引作为患者唯一的标识， 将多个医疗机构中的患者有效地关联在一起， 实现了不同医疗机构之间患者诊疗信息的互联互通， 保证了患者医院不同医疗信息系统中个人信息的完整性和准确性。实现多次门诊或住院期间信息共 享，历次患者的就诊、治疗信息有效地整合， 便于临床、教学活动中展现统一、 完整、连续的患者诊疗信息。

3.1.5.1主索引信息查询

➢可支持以姓名、身份证、电话号码等方式查询患者相关信息， 查询后界面 列出符合条件的患者，点击后可呈现患者相关信息及就诊机构信息等；

➢可提供 API 接口提供患者主索引的调用。

3.1.5.2相似患者管理

➢通过姓名、证件号等条件检索后，可呈现疑似患者与索引患者的匹配度， 如姓名、出生日期、性别、身份证等，并可将不同之处用其他颜色显示或标注；

➢可支持人工判断审核疑似患者，同时对误操作生成的索引进行拆分。

3.1.5.3匹配规则管理

支持可视化配置界面对精确匹配条件进行设置， 可将匹配条件设置为条件组。

3.1.5.4操作记录查看

支持对患者主索引操作历史的查看， 通过操作时间或主索引号的查询即可检 索出该主索引被操作的详细信息。

3.1.5.g隐私数据脱敏

支持根据隐私保护开关设置是否进行数据脱敏。可以对患者姓名、联系人、

身份证、患者手机号、联系人手机、医保卡号、工作单位内容、护照号、港澳通行证号、台湾通行证号、军官证、医疗保险号、邮箱、地址等信息进行不同方式的脱敏。

3.1.5.6系统性能指标

➢数据滚动加载数据时不超过 1 秒；

➢tab 页切换不超过 1 秒；

➢患者记录管理、索引记录管理、相似患者管理、数据匹配日志功能加载时 间不超过 1s。

3.1.5.7患者主索引数据质量

各医疗机构之间或者院内各系统之间患者信息填写质量参差不齐， 并且存在人为误填、漏填等各种情况为了提高主索引数据质量， 患者主索引数据初始化应优先将数据质量好的记录做匹配操作。

3.1.6大数据服务

大数据服务应采用中台架构， 底层是国家健康医疗大数据中心和XX医院院 内数据中心，其汇聚了XX市 211 家医疗机构和 14 家省级医院的数据，形成了 面向业务应用的数据标准业务中台， 数据服务在此之上构建， 通过建设大数据服 务系统， 形成面向业务应用提供数据服务的能力， 健康医疗大数据中心以接口方 式对外提供数据服务。

3.1.6.1数据Adl服务模式

- 可对 API 接口进行统一配置和管理；
- 在应用放调用 API 时， 支持对应用放的授权鉴权服务， 在完成鉴权后才可进行对应 API 的调用；
- 针对部分应用场景需要患者敏感信息脱敏的， API 接口需支持数据加密和脱敏的功能，有效地保证了数据的安全，以及数据的隐私要求；
- 支持数据 API 定义、测试、发布、下线等全生命周期的管理；
- 支持按照 T+0 或 T+1 批量的方式向应用系统推送相关数据；

- 支持患者在 37 家XX市属二级及以上医疗机构近五年历史处方、历史病历、检验报告、检查报告、患者信息等信息的查询， 需在 1 秒内返回相应查询结果，支持不低于 1000TPS 的性能指标。

3.1.6.2数据同步方式

- 支持 API 数据接口同步和异构数据库间的数据同步两种方式；
- 可通过源数据库信息、目标数据库信息、数据同步周期、同步优化参数等 相关信息的配置，有数据同步引擎实现不同数据源之间的数据同步。

3.16.3数据赋能应用

➢为满足互联网医院的业务需求，可支持在一秒内将患者在XX市 37 家二级及以上医疗机构线下 3 个月的就诊信息推送至互利网医院平台；

➢可实现与院前急救系统的对接， 在一秒内将患者历史 5 年内的关键就诊信息推送至院内急救中心，有助于急救中心制定更合理的急救方案；

➢在患者手术前， 可将患者基本健康信息、手术信息等推送至手麻重症系统，有助于医生制定更合理的手术方案。

3.1.6.4数据赋能应用

1、互联网医院

为满足互联网医院的业务需求， 可支持在一秒内将患者在XX市属二级以上 公立医院、以及XX市基层医疗卫生机构 3 个月的就诊信息推送至互利网医院平 台。具体要求如下：

➢推送的数据集包括： 患者基本信息、门诊就诊记录、门诊诊断记录、门诊处方明细、检查记录、检验记录。

➢推送的医疗机构包括： XX市属二级以上公立医院、XX市基层医疗机构。

➢实现所推送数据患者主索引构建。

➢数据时效： T+1。

➢数据真实性：数据需要保证真实性， 数据需要确实为医院产生的业务数据，不存在业务字段数据的篡改及混淆。

➢数据可用性： 提供的数据需要具备可以关联查询， 多次查询等功能， 确保业务数据的关联性。

➢数据安全性：提供的数据需要安全可靠，不存在具备恶意攻击性的数据， 对系统安全造成隐患。

➢数据合规性： 提供的数据不能违反国家要求， 不存在违法信息及恶意传播违禁信息等现象。

2、5G+院前急救

➢可实现与院前急救系统的对接， 在一秒内将患者历史 5 年内的关键就诊信息推送至院内急救中心，有助于急救中心制定更合理的急救方案；

➢推送的数据集包括： 患者基本信息、门诊就诊记录、门诊诊断记录、检查记录、检验记录、住院就诊记录，病案诊断信息，病案手术信息。

➢推送的医疗机构包括： XX市属二级以上公立医院、XX市基层医疗机构。 ➢实现所推送数据患者主索引构建。

➢响应时间要求： 1500ms

➢数据时效： T+1。

➢接口性能要求： 1000tps、

➢数据真实性： 数据需要保证真实性， 数据需要确实为医院产生的业务数据，不存在业务字段数据的篡改及混淆。

➢数据可用性： 提供的数据需要具备可以关联查询， 多次查询等功能， 确保业务数据的关联性。

➢数据安全性：提供的数据需要安全可靠，不存在具备恶意攻击性的数据， 对系统安全造成隐患。

➢数据合规性： 提供的数据不能违反国家要求， 不存在违法信息及恶意传播违禁信息等现象。

3.1.7大数据安全管理体系建设

健康医疗大数据平台需要从技术、管理、服务等方面进行全面的安全设计和建设， 有效提高信息系统的防护、检测、响应、恢复能力， 以抵御不断出现的安全威胁与风险， 保证系统长期稳定可靠的运行； 相应的安全保障体系将在统一的安全策略指导下，充分利用和依托已有网络安全基础设施，通过安全技术体系、

安全管理体系、安全服务体系， 形成集防护、检测、响应、恢复于一体的安全保障体系， 从而实现物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、安全管理，构建可信、可控、可管的安全体系。

3.1.7.1安全区域边界设计

➢可对费授权设备私自连接到内部网络行为进行检查或限制；

➢可对内部用户非授权链接到外部网络的行为进行检查或控制

。

9.3.1.L.1.1边界隔离与访问控制

1、安全风险

边界是信息安全的第一道防线， 所有访问内部应用的数据均会通过网络边界进入内部网络， 随着攻击手段的不断演进， 边界所面临的安全风险越来越高， 频 发突发、隐蔽性强、手段多样、实施体系化的复合型攻击， 已经成为当前网络边 界威胁的主要特征。事实证明， 每一次网络攻击的成功， 都是攻击者通过技术手 段数次突破网络边界防线的过程， 传统的边界防御技术已经不能满足新的边界安 全防护的需求。

2、控制要求

等级保护标准在“安全区域边界”中明确要求：

- “应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通 信；”
- “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； ”
- “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； ”
- “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； ”
- “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； ”
- “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。”

3、控制措施

针对新的边界安全威胁，边界访问控制已经成为基本安全措施，必不可少， 但为了更加有效的应对当前的网络威胁，防火墙设备应当更加智能化、联动化， 以满足安全有效性和防御实时性的切实需求。

当前， 下一代防火墙技术已经逐步成熟， 通过相关功能实现及策略配置， 可 实现上述要求。

各安全区域都应针对自身业务特点设定访问控制策略， 下表表述了各安全区域之间的访问控制关系， 在对各网络安全区域设置安全策略时， 可以此为参考原则进行设置。

9.3.1.L.1.2边界入侵防御

1、安全风险

随着国家信息化的发展， 网络攻击活动也愈演愈烈， 而网络攻击造成的破坏性因信息化程度的高度集中也越来越大。主要呈现如下趋势： 网络应用越来越复杂，单纯的依靠端口识别应用以达到攻击检测的目的不再有效； 网络带宽的快速增长给入侵防护系统的处理能力带来挑战， 仅依靠防火墙这样的边界防护设备实现网络攻击检测已经远远不能满足要求， 具备大流量业务并发处理能力的专业设备尤其重要；除具备针对网络层/传输层的基础攻击防护外， 针对应用层深度识别和防御能力越发重要。

因此， 如何有效的对网络攻击行为、异常行为进行监测防御， 是边界安全的重要一环。

2、控制要求

根据等级保护的要求， 针对“安全区域边界”和“安全计算环境”的防护要求包括：

- “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； ”
- “应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； ”
- “检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警” 。
- “应能够检测到对重要节点进行入侵的行为， 并在发生严重入侵事件时提供报警。”

3、控制措施

在网络区域的边界处， 需要通过部署入侵防御设备/下一代防火墙(防病毒)对网络攻击行为进行检测与阻断，并及时产生报警和详尽的报告。

9.3.1.L.1.3高级威胁攻击检测

1、安全风险

近年来，具备国家和组织背景新型网络攻击日益增多，其中最为典型的为 APT 攻击，而 APT 攻击采用的攻击手法和技术都是未知漏洞(0day)、未知恶意 代码等未知行为， 在这种情况下， 依靠已知特征、已知行为模式进行检测的 IDS、 IPS 在无法预知攻击特征、攻击行为模式的情况下， 理论上就已无法检测 APT 攻 击。

2、控制要求

面对新的安全威胁形势， 新等级保护标准中除了对边界攻击检测能力提出要求外， 还明确提出了对高级威胁攻击和未知攻击的检测、发现能力， 具体要求如下：

“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行为的分析。”

3、控制措施

通过部署专业的 APT 检测设备， 实现对新型网络攻击行为的发现、分析、追溯的能力。

9.3.1.L.1.4网络安全准入

1、安全风险

为了防止企业网络资源不受非法终端接入所引起的各种威胁， 在有效管理用户和终端接入行为的同时， 需采用技术手段保障终端入网的安全可信， 同时达到了规范化地管理计算机终端的目的。

2、控制要求

等级保护标准在“安全区域边界”中要求：

“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”。

即需要对单位的内部网络边界进行管控， 对非授权的连接行为能够发现和限制。

3、控制措施

针对网络层的非授权连接行为管控可以通过网络安全准入系统(NAC)进行 控制，网络安全准入系统可实现以下功能：

(1)安全管理与访问控制

利用网络安全准入系统的动态检测技术和安全策略管理， 可针对接入用户和终端进行网络访问控制功能。不符合安全策略的计算机终端进行隔离， 并友好提示， 提供向导式的安全修复指引。拦截可疑的计算机终端或设备、恶意尝试认证的用户，支持强制下线和账号锁定功能。对接入用户进行动态 VLAN 的分配管理，有效的对网络访问权限进行控制。

(2)终端安全合规检查

网络安全准入系统的安全检查策略会检测终端入网安全状态， 能快速定位发现入网计算机终端的安全合规状态， 并利用其本地防火墙隔离管控技术立即将这个设备与网络上的其它设备隔离起来， 只能够访问修复区， 同时依照策略进行引导修复。对于已授权合规终端， 如发现运行阶段又不符合安全检查策略， 可调用周期检查或定时检查引擎， 对该终端的安全状态进行二次检查， 期间如发现不合规进行再次隔离， 禁止其访问企业核心资源， 可提供安全检查结果详情和全网安全状态统计等日志报表。

(3)访客注册申请

针对外来人员临时性的访问需求， 能够进行访客入网管理， 包括访客用户注册申请、访客认证、用户审批流程， 经管理员审批或系统自动审批后才能认证入网，审批结果可邮件通知用户。

(4)设备例外管理

用户网络中存在大量的哑终端设备， 如：网络打印机、视频会议系统等设备， 并分散在各地， 能够提供设备的白名单管理， 当添加到白名单的合法设备可以直 接接入网络， 反之非法设备不允许接入， 此方式可适应于多种认证技术方式， 如： Portal 和 802.1X 认证方式。

9.3.1.L.1.g违规外联检测

1、安全风险

互联网应用已经渗透到社会生活的每一个角落。互联网的开放性、交互性、

延伸性为人们快速获取知识、即时沟通以及跨地域交流提供了极大的便利； 与此同时， 互联网的开放性与虚拟性也为单位和个人带来巨大安全隐患， 如果不对单位的互联网访问行为加以控制，将导致单位的数据、业务面临安全风险。

2、控制要求

等级保护标准中明确要求：

“应能够对内部用户非授权联到外部网络的行为进行限制或检查”。

因此， 不仅要对私自接入内部网络的终端进行发现和阻断， 还要对内部用户的非授权连接外网的行为进行检查和限制。

3、控制措施

对于终端的非法外联可以通过终端安全管理系统或者采用专业的端口网络 行为管理设备进行控制。终端安全管理系统可对终端的外联端口、外联能力进行 检查和阻断， 网络行为管理设备通过在网络出口处进行安全策略的配置， 限制单 位用户的外联访问行为，具体功能如下：

网络行为管控系统

(1) URL 访问审计与过滤

采用 URL 分类数据库， 通过管理员配置基于 URL 分类的控制策略(策略条件可包括用户、部门、时间段、访问类别、 URL 关键字、网页内容关键字、下载文件类型等)，进行 WEB 访问控制，发现非法访问可进行阻断、记录或报警。

(2) 应用控制

通过应用特征与行为特征对应用进行识别。所谓应用特征， 是指在成序列的数据包的应用层信息中， 存在有规律的字节特征， 它可以唯一地标识某种应用协议，行为特征， 是指连续多个包或者多个并发的网络连接表现出来的某种行为模式具有一定规律性， 通过这些行为模式可以识别特征值不明显的应用类型。通过精细化的控制策略设置，可以实现对单位应用访问的精细化管理。

(3)内容审计和过滤

对内容的审计可以有效控制信息的传播范围， 控制敏感信息的泄露， 避免可能引起的安全风险， 内容审计和过滤包括邮件收发审计和过滤、论坛发帖审计和过滤、搜索引擎关键字审计和过滤、 HTTP 文件传输审计和过滤、 FTP 文件传输审计和过滤等。

(4)共享接入监控

共享接入是指使用 NAT 等技术将一个网络出口共享到多个主机， 共享接入监控能够对接入网络的设备做观察、控制，能够检测到一个用户或 IP 所共享的

终 端数量， 并可以对数量做策略控制， 以达到掌控用户终端数量的目的， 在监控到 用户使用的终端数后，可以对此进行控制，屏蔽该用户的上网流量。

(5)日 志 审 计

能够完整地记录内网用户网络访问的日志， 包括上网时间、网络流量、Web 访问记录、接收与发送的邮件等等。为进一步的查询统计与报表分析提供了完整 的基础信息。

终端安全管理系统

为了防止计算机终端用轻易通过拨号、私设代理、多网卡通讯等非法外联手段，造成内部机密外泄的情况发生，终端安全管理系统提供非法外联管控功能， 可根据探测类型，使用对应的技术手段如域名解析，对传入的 ip 或是网址进行 连接，如果连接成功则根据策略处理措施，进行对应的提示、断网或关机处理。

(1)外联设备控制(可以禁用终端上可能运行的外联设备——冗余有线网 卡、移动数据网卡、 MODEM 设备、 ISDN 设备、 ADSL 设备、 WIFI 及 SSID 例外)

(2)外联能力探测(选择探测方式发现终端是否具有外联能力)

(3) 外联控制措施(发现终端具有外联能力后的处理措施——提示、断网、 关机)

9.3.1.L.1.9边界恶意代码检测

1、安全风险

当前， 病毒的产生速度、种类、危害程度已经发生了巨大的变化， 电子邮件和互联网已经成为网络病毒传播的主要途径， 由于网络传播的快速性， 对于越来越多的混合型病毒和未知病毒更加难以防范， 影响范围也更大， 而病毒一旦进入网络内部植入主机， 往往已经对单位造成了损失， 因此，需要在网络边界处入手， 及时检测处病毒，并切断传播途径，采取更积极主动的防病毒措施。

2、控制要求

根据等级保护要求“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”。

3、控制措施

为了整体投资利益最大化， 本次 IPS 带的防病毒模块来实现， 卫计委专网通过 IPS 在网络边界处进行病毒的检测和阻断。

9.3.1.L.1.L网络安全审计

1、安全风险

随着《网络安全法》的颁布实施， 安全审计已经成为网络安全建设的必要措施，随着威胁的多样化，传统信息安全以“防”为主的思路已经发生重大转变， 在攻击防不胜防的情况下， 持续的监测、快速响应并追踪溯源成为新等级保护体 系下的主要思想，因而，安全审计变得尤为重要。

2、控制要求

《网络安全法》第二十一条之(三)规定“采取监测、记录网络运行状态、 网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月”。

等级保护标准中针对网络安全审计的要求包括：

- “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； ”
- “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；”
- “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”。

3、控制措施

网络安全审计系统通过镜像获取通过核心交换机上流量数据可对整个网络 的流量进行审计分析，可对用户的行为进行审计。包括：

(1)对用户的 HTTP、邮件、 FTP、TELNET 等应用进行审计。

(2)对远程桌面等远程访问行为进行审计。

(3)对用户的网络访问行为进行审计。

(4) 本地日志可以 FTP、USB 等方式导出， 支持将日志发送至外置日志存储系统，确保日志记录满足合规要求。

➢网络安全事件的踪迹一般都分布在网络的边界设备、安全设备、访问控制设备的日志中， 除对网络流量中用户的行为进行审计分析外， 发现网络安全事件 也是网络安全审计的重要目标， 集中安全审计系统通过收集网络设备、安全设备、 服务器、应用系统等的日志信息， 结合网络流量日志进行关联分析， 可以快速发 现网络安全事件，并进行定位和报警。

3.1.7.2安全计算环境设计

➢支持对登陆的用户进行身份标识和鉴别， 身份鉴别信息具有复杂度要求并定期更换；

➢支持登陆失败处理功能， 配置并启用结束会话、限制非法登陆次数和登录超时自动退出等相关措施；

➢支持口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户 进行身份鉴别。

9.3.1.L.2.1主机身份鉴别与访问控制

1、安全风险

信息系统面临的一个主要安全威胁就是身份信息被假冒， 随着攻击技术的发展，对于常见的身份鉴别方式， 如用户名+密码，采用字典攻击等手段进行破解 仅仅需要几分钟甚至更短， 因此， 对于重要的操作系统和应用系统用户的身份鉴 别信息应具有不易被冒用的特点， 采用口令或指纹等生物识别方式加基于密码技 术的身份鉴别手段实现双因素认证，是实现身份安全可靠的重要手段。

所有涉及的系统用户(包括技术支持人员， 如操作人员、网络管理员、系统 程序员以及数据库管理员等)应当具备仅供其个人或单独使用的独一无二的标识 符(即用户 ID)，以便跟踪后续行为，从而责任到人。

2、控制要求

等级保护制度在“安全计算环境”中， 对包括终端和服务器设备操作系统在内的保护对象统一提出了安全保护要求，包括身份鉴别和访问控制要求。

身份鉴别要求包括：

“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； ”

“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； ”

“应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用 户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现”。

访问控制要求包括：

“应对登录的用户分配账号和权限； ”

“应重命名或删除默认账户，修改默认账户的默认口令； ”

“应及时删除或停用多余的、过期的账户，避免共享账户的存在； ”

“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。”

“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；”

“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； ”

“应对重要主体和客体设置安全标记， 并控制主体对有安全标记信息资源的 访问。”

3、控制措施

针对主机的身份鉴别一般可采用堡垒机管理， 堡垒机能够给用户分配唯一的 “网络身份证”，对登录的用户进行身份标识和鉴别， 身份鉴别信息设置复杂度 要求并定期更换。

针对主机访问控制的要求，采用服务器加固系统，并进行以下安全配置：

启用访问控制功能，依据安全策略控制用户对资源的访问；

根据管理用户的角色分配权限， 实现管理用户的权限分离， 仅授予管理用户 所需的最小权限；

严格限制默认帐户的访问权限， 重命名系统默认帐户， 修改这些帐户的默认 口令；

及时删除多余的、过期的帐户，避免共享帐户的存在；

对重要的主机系统采用专业的主机安全加固系统对主机进行整体安全防护， 设置强制安全访问控制策略，从而使操作系统达到 B1 级高安全级别。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：

https://d.book118.com/415143012100011311