医 疗 保 障 影 像 云 标 准

YXY-INF-2025-A1

医保影像云 基础设施技术规范

（征求意见稿）

2025-XX-XX 发布　　2025-XX-XX 实施

国家医疗保障局发布

目次

前言

为规范医保影像云基础设施、网络、安全防护、容灾备份、存储介质处置等，特制定《医保影像云基础设施技术规范》。

本规范按照GB/T 1.1—2020《标准化工作指导 第1部分：标准化文件的结构和起草规定》规定起草。

本规范起草单位：

本规范起草人：

医保影像云 基础设施技术规范

1 范围

本规范明确了医保影像云涉及的物理环境、硬件设备、基础平台、网络架构、安全防护、容灾备份及存储介质处置等方面技术要求。适用于各级医保部门、定点医疗机构、第三方技术服务机构等。

2 规范性引用文件

GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》

GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》

GB 50057-2010 《建筑物防雷设计规范》

GB 50116-2013 《火灾自动报警系统设计规范》

GB 50174-2017 《数据中心设计规范》

GB 50343-2012 《建筑物电子信息系统防雷技术规范》

GB/T31596.4-2015《社会保险术语 第 4 部分:医疗保险》

《全国医疗保障系统核心业务区骨干网络建设指南》 国家医疗保障局（医保网信办〔2019〕3 号）

《医疗保障核心业务区网络安全接入规范》 国家医疗保障局（医保网信办〔2019〕40 号）

3 术语和定义

医保影像云

依托全国医保信息平台，遵循医保技术与业务标准规范，运用云计算、大数据等技术，构建实现影像检查数据全国存储、机构调阅、参保人查阅的数字化服务平台，支撑全国定点医疗机构间医保支付相关影像检查数据的互通共享。

影像数据共享中心（以下简称“共享中心”）

各省对辖区内定点医疗机构产生的影像检查数据进行集中存储、图像质控、动态缓存、数据管理、数据调度的系统。

定点医疗机构

经医疗保险行政管理部门进行审核获得定点资格,并与医疗保险经办机构签订服务协议,为基本医疗保险参保人提供医疗服务的医疗机构。

第三方技术服务机构

为医保影像云建设、运营、维护提供技术支持、系统开发、服务保障等专业化服务的第三方机构。

医疗保障核心业务区网络

由国家医疗保障局统一规划，承载医疗保障核心业务数据交换的专用、安全网络。

医保影像云专网

承载各级医保影像云影像检查数据高效、安全传输与调阅的专用广域网络。

4 物理环境要求

4.1 机房基础

4.1.1 建设等级

数据中心机房规划与建设应遵循GB 50174-2017《数据中心设计规范》相关规定。等级划分要求如下：

a）A级标准：适用于国家医保影像云。

b）B级及以上标准：适用于各省级医保影像云、三级定点医疗机构。

c）C级及以上标准：适用于三级以下定点医疗机构。

4.1.2 功能区域

机房应明确划分用于安装和运行服务器、存储、网络等核心信息技术设备的主机房，用于设备的安装、调试、维护、运行监控和管理的辅助区，用于为主机房和辅助区提供动力支持和安全保障的支持区。

4.1.3 机房选址

a）应远离强振源、强噪声源、强电磁场干扰源、易燃易爆品仓库及高污染源等环境敏感区域；

b）应避开机场、军事基地、政府要害部门、危险品仓库、化工厂、学校等特殊场所及地势低洼区域，周边需具备完善的交通、供电、网络、给排水等基础配套条件；

c）若机房设置在多层或高层建筑内，宜优先选择较低楼层，其楼面承重标准不应低于800kg/㎡，且需避开卫生间、茶水间等存在水管泄漏风险区域的正下方。

4.1.4 温湿度与环境

a）主机房在设备开机运行时，温度应控制在23℃ ± 2℃，相对湿度应控制在40%~60%；

b）应配置专用精密空调系统，确保温湿度稳定，并维持机房内正压。机柜布局宜采用冷热通道方式进行隔离；

c）宜配置具备高效过滤功能的洁净新风机组，以保障机房空气洁净度。

4.1.5 消防设施

a）应配置符合GB 50116-2013《火灾自动报警系统设计规范》要求的极早期火灾自动报警系统；

b）主机房应配置对电子设备无害的气体灭火系统（如IG541、七氟丙烷），并与火灾探测器、空调、门禁等系统进行联动控制；

c）设置气体灭火的机房，应在指定位置配置专用空气呼吸器或氧气呼吸器，并在入口处设置灭火显示灯和声光报警器。

4.1.6 网络布线

a）传输介质：核心主干链路光缆应采用OM3及以上规格的多模光缆或单模光缆；水平链路电缆应采用六类及以上屏蔽/非屏蔽对绞电缆；

b）防火等级：布线电缆应采用CMP（增压级）或CMR（干线级）防火等级，光缆应采用OFNP或OFCP防火等级；

c）走线方式：双绞线和光缆宜采用机柜上方（上走线）桥架或线槽进行布放，并与强电线缆保持安全距离；

d）配线管理：每列机柜宜设置列头配线柜，用于汇聚本列机柜线缆。

4.1.7 不间断电源

a）应配置N+1或2N冗余架构的在线式不间断电源，满载后备时间不少于2小时；

b）核心业务设备应由不间断电源系统供电，并采用双路供电模式；

c）各级医保影像云应配置柴油发电机作为备用电源；

d）三级定点医疗机构可根据实际情况宜配置柴油发电机。

4.1.8 防静电及防雷接地

a）地面应铺设防静电地板，其系统电阻应在$1.0\times10^{6}\sim1.0\times10^{9}\Omega$范围内；

b）应遵循GB 50057-2010 《建筑物防雷设计规范》和GB 50343-2012 《建筑物电子信息系统防雷技术规范》要求，构建有效的多级防雷和等电位联结接地系统。

4.1.9 动力与环境监控系统

应遵循GB/T 22239-2019 《信息安全技术网络安全等级保护基本要求》、GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》，部署机房动力与环境集中监控系统，对UPS、配电柜、精密空调、温湿度、漏水、门禁状态、烟感等进行7×24小时实时监测、数据记录和分级告警。

4.2 安防管理

4.2.1 视频监控

a）监控范围应全面覆盖机房出入口、机房内部通道、核心设备机柜区域，确保无监控死角；

b）视频录像资料保存时间不少于180天，视频清晰度不低于720P，视频帧率不低于25帧，具备红外夜视功能。

4.2.2 出入管理

a）应对机房出入口、监控室、安防设备间、变配电室、UPS电池室、发电机房、动力站房等所有关键区域实施严格物理访问控制；

b）门禁系统宜采用非接触式IC卡、生物特征识别（如指纹、人脸）或组合认证方式。

4.2.3 入侵监控

a）应在机房内部、变配电室、UPS电池室、发电机房、动力站房等关键区域部署红外、微波等入侵探测装置；

b）报警系统应与监控中心联动，并能通过网络、电话或短信等方式及时通知安全管理人员。

5 硬件设备要求

5.1 服务器设备

5.1.1 通用要求

应根据实际部署密度和散热条件，选用1U、2U或4U机架式服务器。

5.1.2 CPU 参数

a）各省医保影像云应满足如下要求：

处理器：应采用多核处理器，支持64位计算，主频不低于2.0GHz。

核心数：单颗物理CPU核心数量不少于16核。

数量配置：台服务器应配置不少于2颗物理CPU。

b）各级定点医疗机构应满足如下要求：

处理器：应采用多核处理器，支持64位计算，主频不低于1.8GHz。

核心数：单颗物理CPU核心数量不少于8核。

5.1.3 内存参数

a）各省医保影像云应满足如下要求：

类型：应采用DDR4 3200MHz或更高规格纠错码内存。

容量：单台服务器内存总容量不低于256GB。

扩展性：内存插槽应具备不少于50%冗余，以满足未来业务增长扩展需求。

b）各级定点医疗机构应满足如下要求：

类型：应采用DDR4 3200MHz或更高规格纠错码内存。

容量：单台服务器内存总容量不低于32GB。

扩展性：内存插槽应具备不少于50%冗余，以满足未来业务增长扩展需求。

5.1.4 硬盘与 RAID 控制器

a）系统盘：应配置2块容量不低于480GB的企业级固态硬盘，并配置为RAID 1；

b）数据盘：可根据业务对I/O性能需求，灵活配置SSD、SAS或NL-SAS硬盘；

c）RAID控制器：应配置独立硬件RAID卡，支持RAID 0/1/5/6/10/50/60，板载缓存不低于2GB，并配备掉电保护模块。

5.1.5 网络接口

a）板载网口：提供不少于2个千兆电口；

b）业务网口：配置独立网络接口卡(NIC)，提供不少于2个10Gb SFP+光口或2个25Gb SFP28光口。

5.1.6 电源与管理

a）电源：应配置1+1冗余热插拔电源，电源效率符合白金级或更高级别认证；

b）管理：应具备独立远程管理端口，支持KVM over IP和远程虚拟介质功能。

5.1.7 GPU 加速服务器

a）GPU卡：应配置支持FP32/FP16/INT8等多种精度计算的高性能计算卡，单卡显存不低于32GB；

b）CPU：应配置与GPU性能相匹配的高主频、高核心数CPU，避免成为性能瓶颈；

c）总线：应支持PCIe 4.0或更高版本的总线，为CPU与GPU之间提供足够的数据传输带宽；

d）散热：应具备针对GPU优化的散热设计，确保在高负载下长期稳定运行。

5.2 存储设备

5.2.1 通用要求

a）架构：可根据业务场景、性能和扩展性要求选用集中式SAN/NAS存储或分布式存储；

b）控制器：应采用全冗余架构，控制器应为Active-Active（双活）模式，确保无单点故障。

5.2.2 控制器参数

a）缓存：单控制器缓存容量不低于64GB；

b）协议：应至少支持FC、iSCSI、NFS、CIFS、S3等协议中的两种，以适应不同应用场景。

5.2.3 端口配置

a）前端端口：每个控制器接口数不少于4个，接口速率不低于16Gb FC端口或10Gb iSCSI端口；

b）后端端口：应采用不低于12Gb/s的SAS 3.0通道连接磁盘柜。

5.2.4 硬盘配置

a）类型：支持SSD、10K/15K RPM SAS、7.2K RPM NL-SAS等多种类型硬盘，并支持在同一存储池中混合配置；

b）RAID模式：应支持RAID 0/1/5/6/10/50/60及动态RAID/纠删码技术。

5.2.5 系统功能

a）数据保护：应具备快照、克隆、远程复制、双活、自动精简配置、服务质量控制等高级数据服务功能；

b）静态数据加密：所有存储系统应启用静态数据加密功能，宜支持密钥管理互操作性协议。

5.2.6 存储分层策略

自影像检查完成时起，门（急）诊影像检查数据须存储15年，住院影像检查数据须存储30年，影像检查数据可采用分层存储策略：

a）在线存储：用于存储近期（如3年内）影像数据，应采用全闪存阵列或SSD/SAS混合阵列；

b）近线存储：用于存储中长期（如3-5年）影像数据，宜采用大容量NL-SAS磁盘阵列；

c）离线归档：用于长期（5年-15年及以上）影像数据归档，宜采用磁带库、虚拟带库或蓝光光盘库等低成本、高持久性介质。

5.3 网络设备

5.3.1 核心交换机

a）架构：采用模块化、CLOS无阻塞交换架构，主控、交换网板、电源、风扇等关键部件应支持冗余和热插拔；

b）性能：整机交换容量不低于32Tbps，包转发率不低于9600Mpps；

c）端口：支持高密度的10Gb/25Gb/40Gb/100Gb自适应接口，满足不同速率接入需求；

d）功能：支持VLAN、VXLAN、STP、OSPF、BGP等二、三层网络协议，并支持高可用、虚拟化堆叠技术。

5.3.2 汇聚交换机

a）性能：整机交换容量不低于2.5Tbps，包转发率不低于480Mpps；

b）端口：提供高密度的千兆和万兆光/电接口，上行接口速率不低于40Gbps；

c）功能：支持完善的二层特性和静态路由、RIP、OSPF等三层路由协议；

d）可靠性：关键部件如电源、风扇支持冗余和热插拔。

5.3.3 接入交换机

a）性能：整机交换容量不低于500Gbps，包转发率不低于100Mpps；

b）端口：下行提供不少于24个100/1000Mbps自适应电口；上行提供不少于4个10Gb SFP+光口；

c）功能：支持VLAN、链路聚合（LACP）、端口安全、ACL等二层安全与管理特性；

d）电源：宜采用冗余可插拔电源模块，提升设备可靠性。

5.3.4 广域网路由器

a）架构：采用支持双主控、双电源等冗余设计的模块化路由器；

b）性能：包转发性能应能满足专网和互联网出口总带宽的线速转发需求；

c）功能：支持BGP、OSPF等高级路由协议，具备强大的网络地址转换（NAT）能力和完善的服务质量（QoS）策略，能够对不同业务流量进行优先级标记、带宽保障和拥塞管理；

d）安全：支持主流安全加密传输技术、访问控制列表（ACL）等基础安全功能。

6 基础平台要求

6.1 服务器虚拟化

a）具备虚拟化集群管理、虚拟机在线迁移、在线克隆等核心功能；

b）具备宿主机故障时，虚拟机自动重启或迁移的高可用性（HA）功能；

c）宜具备分布式资源调度能力，实现计算资源的动态负载均衡；

d）宜支持网络虚拟化，实现灵活的网络策略定义和微分段。

6.2 存储虚拟化

a）采用分布式架构，实现单节点故障不影响数据存储的完整性和业务连续性；

b）支持统一提供块、文件、对象等多种存储服务类型。

7 云服务要求

若采用私有云或政务云服务,其提供的服务能力应不低于本规范中对私有化部署相应要求。

7.1 云服务器

支持提供通用型、计算优化型、内存优化型、存储优化型、GPU加速型等多种实例规格。

7.2 云存储

a）类型：支持提供块存储、文件存储、对象存储等多种存储类型；

b）对象存储可用性：服务可用性不低于99.99%，数据持久性不低于99.999999%；

c）静态数据加密：云存储服务宜启用静态数据加密功能。

7.3 云备份服务

a）提供对云服务器、云硬盘等资源的快照或备份服务；

b）支持按策略自动执行备份任务，并能将数据恢复到任意备份点。

7.4 集中监控管理

建设集中统一的监控平台，对所有服务器、网络设备、存储设备、基础软件及机房环境的核心运行指标（如CPU使用率、内存占用、网络流量、磁盘I/O、应用响应时间、温度）进行7×24小时不间断监控和历史数据分析，并建立分级告警机制与通知流程。

8 网络要求

8.1 总体建设要求

a）影像云索引数据通过医疗保障核心业务区网络上传至国家医保信息平台；

b）各省医保影像云、定点医疗机构影像检查数据传输应通过新建的医保影像云专网进行；

c）医疗保障核心业务区网络与医保影像云专网应实现逻辑隔离。

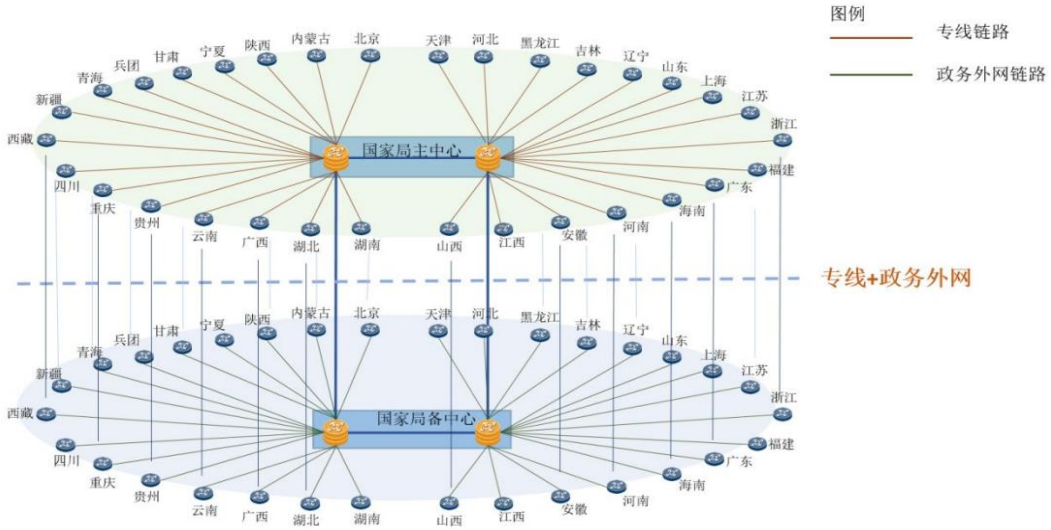

图 1　医保影像云专网组网示意图

8.2　医保影像云专网

8.2.1　网络接入

各省医保影像云应依据《全国医疗保障系统核心业务区骨干网络建设指南》（医保网信办〔2019〕3 号）和《医疗保障核心业务区网络安全接入规范》（医保网信办〔2019〕40 号），完成医保影像云专网安全、合规接入。

各省日均异地就诊转入或转出量超过 2 万人次时，应部署主备冗余线路。

8.2.2　性能指标

a）网络平均延迟≤100ms；

b）平均丢包率≤0.1%；

c）全年网络可用性≥99.99%。

8.2.3　专线带宽

各省医保影像云应依据日均异地就诊转入和转出人口数量中的较高值，参照下表进行专线带宽基线选型。

表 1　医保影像云专线带宽要求对照表

日均异地就诊转入/转出人数	最低网络带宽要求（Mbps）
≥100000	≥4200
≥80000	≥3300
≥50000	≥2100
≥30000	≥1200
≥10000	≥400
≥5000	≥200
≥2000	≥100

注：表中未列出数值，可参照已有数据按比例进行估算。

8.3 定点医疗机构网络

8.3.1 性能指标

定点医疗机构接入医保影像云专线网络，其性能指标应符合8.3.2章节要求。

8.3.2 专线带宽

定点医疗机构应依据日均影像数据上传量（参照表2）和日均院内就诊量（参照表3），分别估算上行与下行带宽需求，并按两者中的较高值进行专线带宽选型。

表 2 定点医疗机构专线上行带宽要求对照表

日均影像数据量	最低上行网络带宽要求(Mbps)
≥1000GB	≥900
≥800GB	≥700
≥500GB	≥450
≥300GB	≥250
≥200GB	≥200
≥100GB	≥100
≥50GB	≥50

注：表中未列出数值，可参照已有数据按比例进行估算。

表 3 定点医疗机构专线下行带宽要求对照表

日均就诊量	最低下行网络带宽要求(Mbps)
≥100000	≥3050
≥80000	≥2450
≥50000	≥1500
≥30000	≥900
≥10000	≥300
≥5000	≥150
≥2000	≥50

注：表中未列出数值，可参照已有数据按比例进行估算。

8.4 医保影像云互联网

各省医保影像云应根据本省日均检查量评估互联网带宽需求,并参照下表进行互联网带宽选型。互联网出口宜采用BGP多线方案，以提升访问质量和可用性。

表 4　医保影像云互联网带宽要求对照表

日均检查量	最低网络带宽要求(Mbps)
≥100000	≥1850
≥80000	≥1450
≥50000	≥900
≥30000	≥550
≥10000	≥200
≥5000	≥100

注：表中未列出数值，可参照已有数据按比例进行估算。

9　安全防护要求

9.1　医保影像云数据中心安全

9.1.1　网络防火墙

数据中心网络边界、互联网出口及内部核心区域边界部署高性能网络防火墙，用于访问控制、区域隔离和威胁防护。

9.1.2　入侵防御系统

具备对网络攻击行为的深度检测、实时分析和主动防御能力。

9.1.3　Web 应用防火墙

具备对SQL注入、跨站脚本（XSS）、文件上传漏洞等常见Web攻击的防护能力。

9.1.4　日志审计系统

能够对网络设备、安全设备、服务器、操作系统、数据库和应用等所有IT组件的日志进行集中采集、范式化、关联分析和安全存储。

日志保存时间应不少于180天。

9.1.5　数据库审计系统

对数据库的访问操作进行独立监控、记录和分析，并对SQL注入、越权访问等高危操作进行实时告警。

9.1.6　运维审计系统

对所有运维人员（内部员工、外部合作方）的远程访问进行统一身份认证、权限控制、操作审计和会话录像回放。

9.1.7　漏洞扫描设备

具备对主机、网络设备、Web应用、数据库等资产进行定期自动化漏洞扫描能力，并提供修复建议和风险趋势报告。

9.1.8 安全信息与事件管理平台

宜部署安全信息与事件管理平台，对各类安全日志和事件进行集中关联分析，整合威胁情报，实现威胁的统一监测、预警、研判和响应处置。

9.1.9 数据防泄漏系统

宜在网络出口和终端，部署数据防泄漏系统，对包含个人身份信息、影像诊断报告等敏感数据的外发行为进行深度内容检测、监控和阻断。

9.2 网络边界与通信安全

9.2.1 网络隔离

通过部署网络防火墙或安全隔离网闸，实现不同安全等级网络区域（如互联网接入区、应用服务区、数据核心区、运维管理区）之间的有效隔离和访问控制。

9.2.2 传输安全

a）业务系统之间涉及敏感数据传输时，应采用基于国密算法或TLS 1.2及以上协议，并禁用已知存在漏洞的加密套件；

b）个人敏感信息在传输过程中，应进行字段级加密。

9.2.3 流量控制

宜部署流量控制设备，对网络流量进行分析和管控，具备用户行为分析、应用带宽限制、应用带宽保障等功能。

9.3 终端安全

9.3.1 终端认证

终端接入系统时，应采用至少两种组合鉴别技术（如密码+短信验证码、密码+数字证书）进行身份认证，即多因素认证。

9.3.2 传输加密

终端设备通过公共网络访问业务系统时，应使用基于国密算法或TLS 1.2及以上协议对传输数据进行加密。

9.3.3 终端防护

所有接入网络的终端（包括服务器和个人电脑）应安装统一管理的防病毒软件，并宜具备终端侦测与响应能力。

9.4 密钥管理安全

应建立完善的密钥全生命周期管理体系，包括密钥生成、分发、存储、轮换和销毁。核心数据加密，宜采用经过国家密码管理部门认证的硬件加密机进行密钥安全保管。

9.5 身份与访问管理

9.5.1 统一身份认证

应建立集中式身份管理系统，对所有用户（内部员工、外部合作方）和系统账号进行统一生命周期管理（创建、授权、禁用、删除）。

9.5.2 多因素认证

所有对生产环境访问，尤其是涉及特权账号访问（如服务器SSH、数据库登录、云平台控制台），应强制启用多因素认证。

9.5.3 权限访问控制

应严格遵循“最小权限”和“职责分离”原则，实施基于角色的访问控制，确保每个用户仅拥有其完成本职工作所必需最小权限集合，并定期（如每半年）对用户权限进行审查。

9.6 安全运营与审计

9.6.1 定期安全评估

应定期（至少每年一次）委托具备资质的第三方机构开展渗透测试和安全评估，从攻击者视角检验系统实际安全防护能力，并对发现风险进行跟踪修复。

9.6.2 应急响应

应建立正式的安全事件应急响应预案和响应团队，明确事件上报、研判、处置、溯源和恢复流程。宜定期组织应急响应演练，确保预案可行性和团队熟练度。

9.6.3 配置与补丁管理

应建立正式的流程和工具，对所有IT资产的安全配置基线进行统一管理和合规性检查，并对机构发布的高危安全补丁进行评估、测试和及时部署。

10 容灾备份要求

10.1 容灾目标

恢复时间目标（RTO）：关键业务系统RTO不超过4小时。

恢复点目标（RPO）：关键业务数据RPO不超过1小时。

10.2 数据备份

医保影像云应对核心业务数据和系统配置进行定期、自动化本地备份，可采用数据快照、同/异步复制等技术。

11 存储介质处置要求

存储个人敏感信息或重要业务数据的介质在报废、维修或转让前，应通过不可逆的数据擦除（如多次覆写）或物理销毁（如消磁、粉碎）方式，确保其存储的数据无法被任何技术手段恢复。应制定数据销毁策略和流程，并对销毁过程进行记录和审计。

附录 1

参 考 文 献

[1] GB/T 28827.1-2012 《信息技术服务 运行维护 第1部分：通用要求》

[2]GB 50019-2015 《工业建筑供暖通风与空气调节设计规范》

[3]GB 50311-2016 《综合布线系统工程设计规范》

[4]《全国医院信息化建设标准与规范》（试行）国家卫生健康委办公厅 国卫办规划发〔2018〕4号

[5]《全国公共卫生信息化建设标准与规范》（试行）国家卫生健康委办公厅 国家中医药局办公室 （国卫办规划发〔2020〕21号）