地市级电子政务网络市域安全一体化运营研究与实践

吴洁慧

（中国电信股份有限公司湖州分公司　浙江　湖州　313000）

【摘　要】2021 年初，浙江在全省部署开展数字化改革，从整体上推动省域经济社会发展和治理能力的变革，此举全国率先。随着新科技革命和产业数字化变革蓬勃发展，网络安全运营不再是孤立的，而是呈现整体性、系统性、关联性趋势，数字经济发展和网络安全保障成为并驾齐驱的“两个轮子”，缺一不可。为此，本文以浙江省湖州市为例，梳理该市电子政务网网络安全现状、困境和发展规划等，结合实际探讨研究建设地市级电子政务网络市域安全一体化体系的可行性，并付之实施形成标杆。本研究报告还可为浙江省乃至全国的地市级市域网络安全体系建设提供借鉴。

【关键词】电子政务网络；网络安全；体系建设运营

一、湖州市电子政务网络安全现状与问题

（一）湖州市域网络安全保障发展优势

1. 安全基础设施建设相对完善

在云网应用安全支撑方面，湖州市大数据发展管理局（以下简称“市大数据局”）依托政务云云上安全资源池的安全防护能力和安全服务团队快速的应急处置能力，有效提高了政务云及云上租户安全保障水平；依托电子政务网有效整合部门专网，规范网络出口，实行边界安全全防护；在数据安全层面，市大数据局联合第三方安全服务企业，共同研究并制定数据安全防护方案与策略并逐步落实，已具备传输安全和 SSL/VPN 技术、数据恢复技术、基于日志安全审计和静态脱敏等保障技术，保护数据安全。

2. 整体安全防护意识明显提高

市大数据局相应制定了 18 项内控安全管理制度。随着湖州市数字化改革工作的进一步推进，通过业务流程再造实现跨层级、跨地域、跨系统、跨部门、跨业务的高效协同。各单位也意识到，在大量公共数据归集整合以及共享开放的过程中，数据应用的场景复杂多样，更多的业务应用从原先的单部门应用向跨部门的融合业务转变，业务和数据的融合加大了数据安全防护的难度[1]。

3. 信息安全生态发展健康

湖州市正逐步建立有利于安全企业和安全人才引进的政策体系，鼓励本土信息安全企业研发核心安全技术、创新安全产品功能。充分发挥政府的桥梁与协调作用，主动吸纳和整合中国电信湖州分公司、湖州市大数据运营有限公司、安恒信息等本省、市知名的平台提供商、数据运营商和安全服务商能力，明确各服务商的安全角色和职责要求，互通有无，发挥专长，促进湖州市整体信息安全生态健康发展。

目前已成立湖州智慧城市研究院，下设安全组，结合行业内安全专家与本地企业的优秀人才共同为湖州数字化改革与智慧城市建设进行赋能。

（二）亟需解决的问题

1. 网络安全顶层设计与标准不够完善

目前湖州市尚未形成完善的电子政务领域网络安全保障总体工作方案，需要结合湖州市数字化改革发展的现状，编制顶层设计体系化的政策制度文件[2]。

2. 安全管理制度与流程机制欠完善

尽管湖州市单位都结合等级保护相关要求制定了本单位的制度与流程，但主要以传统网络与信息系统安全管理规范要求为主，不能很好的适应数据开放共享业务对数据在流通过程中的安全管控需要[3]。

3. 大数据管理部门安全监管职能未能有效发挥

市、区县各大数据发展管理局在履行自身的安全监管职责时，监管的方式也主要通过周期性的安全抽查和建设服务方周期性的汇报实现，且因为人员编制原因，并不具备专门的信息安全监管的队伍，无法有效实施和推进监管工作。

作者简介：吴洁慧（1979.06-），男，汉族，浙江湖州，本科，工程师，研究方向：通信信息，DICT、云计算、物联网、5G、大数据、网信安全等。

4. 安全运营综合协调指挥机制还未形成

缺乏全市一体化、自动化的安全运营机制，无法有效实现市网信、公安、大数据局以及其下辖行政区公共数据服务与使用单位、信息安全支撑单位等组织在网络安全上的自动化协作、互通，尚未建立市域电子政务一体化的监测预警、信息通报、应急处置、追踪溯源等相关机制[4]。

二、市域安全一体化建设框架

（一）安全保障总体目标

以安全运营中心为总抓手，深入落实“实战有效、体系完善、常态保护、综合治理”的安全保障总体目标。实战有效，必须保障关键业务不失陷、真实攻击能溯源、简单有效高可用。体系完善，落实各单位网络安全等级保护、关键信息基础设施保护、信息安全管理体系。常态保护，基于全链路安全监管平台能力，参照安全威胁情报，落实市域电子政务一体化安全运营中心的常态化保护。综合治理，强化监管职能，基于框架指导，评估洞察，落实综合监管，完善协同防御。

（二）总体架构设计

按照“大安全、大运营、大协同”的建设思路，市大数据局统筹湖州市电子政务网络建设中的政务云安全、网络安全、边界安全、终端安全、数据安全和应用安全，中国电信湖州分公司在市大数据局的指导下，构建安全保障总体目标，打造“1231”的市域安全一体化安全保障总体框架体系，即一个总体目标、两项理论支撑建设、构建三大安全体系，通过从技术层面、管理层面、运营层面，打造一个基于云、网、端、数、用、边全链路的市域一体化数字安全运营中心。

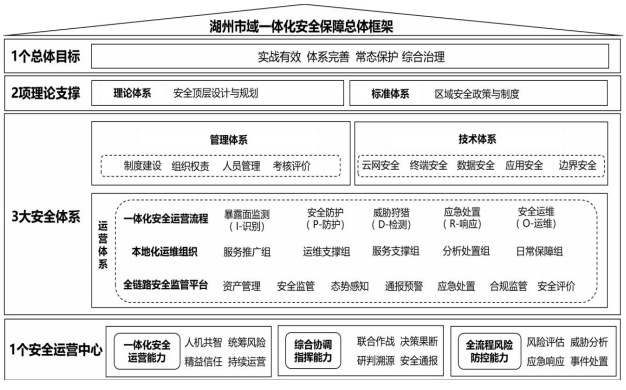

图 1 湖州市域一体化安全保障总体框架

（三）两项理论支撑

1. 顶层设计

在遵循国家安全相关政策和国家标准的基础上，制定湖州市数字化改革安全保护方面的顶层设计与指导性方案《湖州市政务网络市域安全一体化总体工作方案》，约束和规范各单位开展数字化改革业务过程中的行为。明确湖州市网络安全体系的总体策略和方针，完善一体化智能化公共数据平台安全建设的要求，实现安全防护的总体目标。

2. 标准体系

湖州市大数据局要全面贯彻《浙江省数字化改革总体方案》中“标准规范体系”相关要求，在省大数据局的指导下联合“湖州市智慧城市研究院”加快研究编制《安全运营中心工作管理规范》和《数据分级安全建设指南》，标准建设内容如下：

①《安全运营中心工作管理规范》：规定一体化安全运营中心所使用的服务与人员、技术与工具、机制与流程。明确其覆盖范围涉及到市域范围电子政务外网的“云、网、端、数、用、边”，为县级安全运营中心的建设提供指导和参考。

②《数据分级安全建设指南》：基于当前浙江省出台的 DB33/T 2351-2021《数字化改革 公共数据分类分级指南》，从组织管理、技术保障、制度建设、评价考核等维度对不同级别的数据安全保障措施进行明确，为数据分级后的数据安全保障与落地实施提供指导。

3. 三大安全体系

①管理体系：构建市、区县一体化的安全管理组织架构，明确市、区县大数据局及单位和各服务方安全管理职责，形成各级网络安全专职管理机构的工作重点，确保安全管理方针、策略、制度的有效实施，实现对全市安全风险的有效管理和监督。加强人员安全管理技能培养，满足复杂数据环境下的安全管理职能要求。

②技术体系：市域层面，通过运营中心将各类安全产品的安全能力进行解耦，采用集约化的方式将安全能力统一集成为安全基础资源，并通过标准接口对政府及公共服务单位提供开放、按需、弹性的安全资源服务，利用大数据和人工智能技术构建智能化的安全防护体系。

在区县与各单位层面，应当以相关法律法规以及本方案的相关建设要求为指导，借助市域及区域运营中心的能力或安全资源的集约化能力积极推进业务系统上云以及相关系统的安全保障能

力建设，扎实完成本单位相关系统的网络与数据安全能力建设。

③运营体系：建立湖州市域一体化数字安全运营中心，形成本地化安全运营团队与组织。结合技术体系制订统一的信息安全策略。在规范、统一的平台上有机整合系统内部各种安全技术和产品，同时，使技术因素、策略因素以及人员因素能够更加紧密地结合在一起，突出安全运营在安全保障中的重要地位。开展安全运营服务工作，进行资产测绘与评估、安全巡检与加固、安全监管监测、通报预警与处置，让安全运营服务渗透到一体化智能化公共数据平台以及各类政务应用建设的每一个环节。以安全评价考核收尾，将安全运营整合成一个有机的运营整体，持续优化从而达到动态运营的效果。

4. 一个安全运营中心

①一体化安全运营能力：以数字安全运营中心为总抓手，整合第三方安全厂商，整合市域安全数据资源、整合市域安全软硬件与产品服务能力，构建人机共智、安全能力协同、风险协同防范的支撑体系。理清安全职责边界，合理划分管理职责，落实安全责任制，充分考虑各参与方在安全管理工作中的互补性，建立各参与方的联动协作机制。

进一步汇集安全大数据，从多个维度提供大数据安全分析结果，为研判、决策及重要时期的网络安全保障工作提供有效支撑，面对网络与数据安全事件、威胁，能够快速组织、高效处置，形成事前预警通报，事中防护应急，事后监督整改的安全运营闭环。

②综合协调指挥能力：联合政府单位、监管单位、研究机构、第三方服务商协同作战，对安全事件及时通报、取证溯源数据留存和分析，并立即处置，打造全方位、立体化综合协调指挥能力。通过将安全运营工作流程与浙政钉体系打通，赋能其组织架构体系。将湖州市电子政务相关单位的责任人、管理人员及相关角色进行有效划分，让安全运营过程当中所发现的安全告警、事件、情报、态势可以通过在线自动化的方式快速传达至相关单位进行处置与分析。同时，将区域整体安全事件的处置情况、进度情况、态势情况通报给区域网信部门和公安部门，形成联合作战体系。

③全流程风险防控能力：建立从云到端全链路安全监测能力、防护能力，通过安全风险评估－威胁分析－应急响应－事件处置构建全流程闭环的事件处置流程，提升政务网络安全监测能力和风险防控能力。聚焦湖州市政务云、政务外网、边界、终端、数据、应用的安全保障，结合安全技术保障体系，实现政务云、政务外网、边界、终端、数据全生命周期流转以及应用的安全防护。利用运营中心打造一体化的安全资源服务体系，将安全保障与运营技术能力服务化，实现按需、弹性的分配安全资源服务给各单位用户。同时，利用安全监管措施对安全处置流程各个阶段的安全保障工作和执行情况进行监督管理，确保安全策略在技术环节得到正确执行，相关规章制度在技术层面得到有效的支撑体现。

三、市域安全一体化建设内容

（一）安全管理体系建设

1. 市域安全管理组织建设

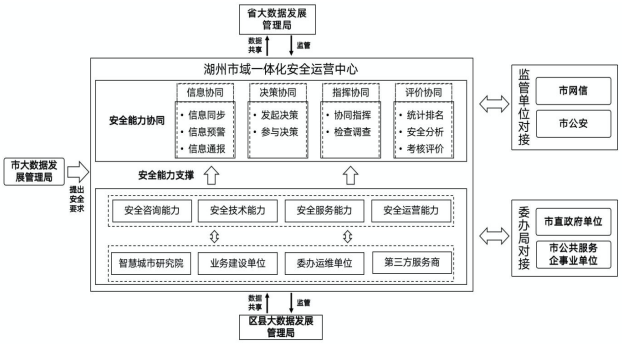

图 2 市域一体化数字安全运营中心在全市管理组织中的定位

借助重点支撑单位智慧城市研究院、业务建设单位、委办运维单位、第三方服务商等提供的安全咨询能力、安全技术能力、安全服务能力和安全运营能力形成安全能力支撑。通过将这些安全能力综合使用，构建信息协同、决策协同、指挥协同和科学评价的安全运营机制。运营中心在市大数据局的统一领导下向上对接省大数据局，向下对接各区县大数据局。同时横向对接监管单位市网信办和市公安局，以及市直政府单位、市公共服务企事业单位等，形成一体化安全管理组织。

2. 各单位安全管理组织建设

按照安全决策层、管理层、执行层和监审层的设计原则，组建本单位的安全管理组织。湖州市各单位落实安全责任体系，需由专门的组织与人员承担网络安全管理工作。各单位的网络安全工作要有一个决策层进行统筹决策，安全决策层由单位主要负责人和相应处室安全负责人共同组成，单位安全分管领导担任首席安全官。

安全管理层，应当由各单位业务、信息化等相关处室的主要负责人承担相关职责。负责按照决策层制定的管理目标、方针和策略制定本单位的安全管理制度规程，并负责具体的执行和落地。建立合理的分工机制，尽量将不同的工作岗位分配给不同的执行层人员来担任，权力不能过于集中在某个人或某些人手里，应相互牵制、相互制约。

安全执行层，是开展具体日常安全管理工作的人员、包括网络管理人员、数据资源管理人员、安全管理人员、第三方服务商等。

安全监审层，在具备初步的安全管理基础上，邀请具备相关监管能力的第三方机构，实现对外包运营单位的业务建设过程当中的安全漏洞监管、安全操作监管、策略执行监管、异常行为监管、安全管理监管、安全合规监管等，定期输出安全监管报告，实现对所有外包运营单位安全评价管理及安全考核管理，监督外包运营单位的运营活动和安全活动，提升外包运营单位的运营服务质量。

（二）安全技术体系建设

1. 政务云安全建设

强化政务云平台安全合规建设。市、区县大数据局所辖政务云应当满足等级保护 2.0 云计算安全扩展要求三级并完成测评。在此基础上结合政务云平台安全技术要求,可信云安全技术要求,建立可信、可靠、安全的政务云平台，提供一体化的、主动的、纵深的安全保障体系，为各单位云租户尽快上云提供安全基础。

加强政务云租户安全建设。市、区县大数据局以运营中心安全能力为基础为本地政务云上各个云租户提供可按需申请及部署的安全产品资源池，并建立相关安全产品和服务资源节点，同时协助各单位进行产品的部署和服务的申请及交付，为云上租户提供一站式的信息安全保障。

2. 政务外网及政务外网边界安全建设

①政务外网区域边界隔离防护。市、区县大数据局以及各单位政务外网安全技术保障设计应当遵循国家电子政务和等级保护的要求,利用“一个中心，三重防护”即“一个安全运营中心，安全通信网络、安全区域边界和安全计算环境”的保障理念进行设计。在进行各类政务系统和应用的安全保障设计时，需要对政务信息系统进行安全控制域的划分（私网、内外网、DMZ 区），确定要保护的计算环境、区域边界和通信网络，并根据安全控制域内保护对象来分别确定各个环节的保护强度，从而来设计不同的安全防护系统。同时应在本级政务外网边界部署相应的安全防护设备，配置访问控制策略，严格控制外部网络对业务系统信息资源的访问，确保网络和信息系统自身的安全。在安全管控技术措施的选择上，需要在满足合规的基本要求基础上，针对 APT 等新型恶意攻击进行有效防护，具体安全保障措施包括但不限于以下控制措施:如访问控制、异常流量检测、抗 DDoS、APT 防护、安全审计、入侵防御、可信接入、恶意代码防护、流量检测等。

②政务外网区域外联监测。市大数据局统筹政务外网的外联监测机制，通过建立外联监测平台对政务网的外联行为进行实时监测并及时通报相关单位进行整改。各单位要严格控制本单位政务网内系统及终端的外联行为。

③政务云上边界安全防护。市、区县大数据局需要针对各单位云上业务系统，通过云平台提供基于东西向流量的安全管控措施，实现不同区域、部门之间的安全隔离。同时，云服务商需要做好与安全行业内优秀信息安全企业的对接，建立云安全资源池，借助云上安全资源池的安全产品服务化能力，为各单位用户提供定制化的安全边界类管控产品，让每个云上的用户可以根据需求去设计自身的安全边界保障机制。

④网络安全态势感知系统建设。目前湖州市电子政务网络中包含有大量的网络设备、服务器、业务系统等，同时随着安全体系的逐步完善，还会增加大量的安全设备。这些数量庞大的网络设备、安全设备在日常运行中会产生大量的安全信息、告警信息，同时又彼此独立，成为一个个的安全孤岛，传统分散的管理方式效率低下而且无法抓取重点信息。为了实现对网络安全资源的统一管理，提高安全事故发现的时效性和处理的效率，市大数据局需要建立网络安全态势感知系统（大数据日志分析平台、阿尔法大数据平台），对区域内政务网络资产情况、风险情况、事件情况、告警情况进行整体态势分析，并依赖态势感知系统、开展通报预警、应急处置等相关技术支撑和运营工作。

3. 终端安全建设

①建设终端安全准入机制。各单位应该配合市、区县大数据局完成准入控制系统的安装与策略制

定，制定本单位的网络准入流程策略，对接入到本单位的内部网络中的临时设备或固定资产进行管理控制，便于固定资产的集中管理和临时设备的有限交互，保证内部网络的安全。同时需结合国产化进程完善国产化终端安全准入控制机制。

②建设终端安全防护机制。各单位配合市、区县大数据局完善本单位终端安全防护机制，通过防病毒、终端入侵防御功能构建立体化终端安全防护体系。同时需结合国产化进程完善国产化终端安全防护机制。

4. 数据安全建设

（1）建立数据安全全生命周期保障机制。在公共数据安全保障的初始阶段，要围绕以数据为核心，开展公共数据治理工作，包括数据分级分类等工作，为后期数据的安全治理与保障提供环境方面的可行性支撑。在保障阶段结合数据生命周期过程安全要求，着重从以下几个方面进行技术体系的设计和保障。

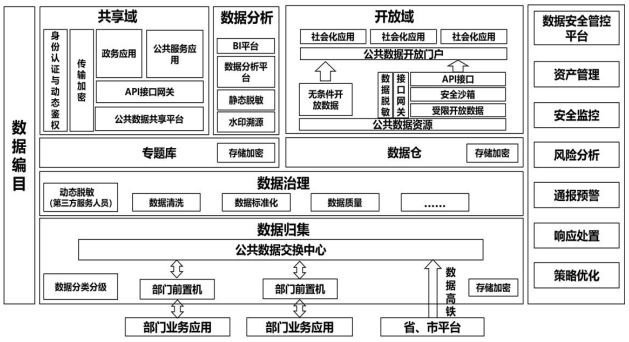

图 3 数据安全全生命周期保障机制

①数据采集阶段，各单位应当重点从数据的合规收集和质量监控、采集数据的分级分类和分级防护、数据清洗转换与加载过程中的完整性与可用性保护等方面进行安全设计。

②数据传输阶段，各单位应当通过利用加密、签名、鉴别和认证等机制对传输中的敏感数据进行安全防护，防止传输过程中可能引发的敏感数据泄漏和数据传输双方对身份的抵赖。

③数据存储阶段，各单位应当建立可伸缩的弹性存储架构，执行严格的数据访问控制策略，防止对存储数据的未授权访问。

④数据处理阶段，通过建立数据脱敏和溯源机制，保障敏感数据和个人信息的泄露防护以及对数据的正当使用（批量取数的流程管控）。

⑤数据共享交换阶段，市、区县大数据局应当通过对数据导入导出、共享、发布环节的监控策略设计，实现对数据交换过程中可能存在的数据滥用、数据泄漏等安全风险的防控。

⑥数据销毁阶段，各单位应当通过建立规范的数据和介质销毁规程，采用合适的销毁工具来防止可能引发的数据泄露风险。

⑦数据开放阶段，市、区县大数据局在数据开放过程当中，应当建立严格的数据开放规范和准则，采用技术工具对开放数据进行内容的识别和监控，并及时告警。

（2）建设数据安全管控平台。市、区县大数据局构建数据安全管控平台，实现对数据安全风险的整体态势感知，对数据资产进行实时风险监测和通报预警，对数据流转过程进行风险监测和预警、对数据用户的操作行为进行监控和审计，实现整体安全风险预警通报能力。对数据资产的采集、处理等管理实现数据质量评估以及数据资产地图等能力。建立敏感数据流转风险监测预警机制，实现敏感数据的分级分类，实现公共数据平台的权限监控，实现数据操作行为的告警。在内部数据流转过程中，实现数据过程的溯源，实现数据访问操作行为的监督审核，实现数据操作的分权分级、合理合规，实现高危操作的数据日志审计。

5. 应用安全建设

①互联网应用安全监测与防护。各单位互联网应用需要将域名指向云端 SaaS 化应用安全监测与保障平台，为其提供安全防护、DDos 安全防护、内容监测、可用性监测等能力。

②未入云应用安全防护。各单位应完成未入云的本地化应用的安全防护建设，通过主动防护建设，防止 Web 服务器受到来自外部的攻击、非法控制和篡改等，同时及时拦截木马、病毒传播等，有效保障应用系统的安全运行。

③建设统一密码服务平台。市大数据局负责本地区统一密码服务平台建设，基于标准国密算法为本市电子政务信息系统提供国产商用密码基础服务。

④重要系统商用密码应用安全性评估。符合等保三级建设的业务系统需要按照 GM/T 0054-2018《信息系统密码应用基本要求》完善本地政务信息系统在规划阶段、建设阶段和运行阶段的密码应用安全建设并完成密码应用安全性评估。

⑤上云安全检查。各单位上云业务系统在入云前需委托安全运营中心对系统进行漏洞扫描、渗透测试和代码审计，实现业务系统安全评审，对于没有通过的单位需要进行整改，且合格后才可以上云。

⑥入云后持续安全保障。各单位在所属业务系统入云后，应马上进行开展该系统安全等级定级，同时根据安全等级要求通过安全运营中心部署相适应的安全防护产品，并完成安全测评工作。三个月内未完成定级的业务系统将被下架。各单位可借助相关安全工具周期性开展云上应用的安全风险评估与安全自查工作，市、区县大数据局将定期对云上业务系统进行安全抽查，确保系统安全运行。

（三）安全运营体系建设

1. 市域一体化数字安全运营中心的定位

①运营中心是联动市、区县网络安全工作的总枢纽。运营中心按照“市域一体、上下贯通、协调联动、能力互补”的模式，为全市网络安全和数据安全提供技术保障服务和安全运营服务。

②运营中心是开展一体化网络安全保障工作的总抓手。是安全保障技术工具、管理制度、运营服务输出的主要载体。是安全保障市、区县电子政务外网以及基于政务外网运行的系统和产生数据资源的网络安全咨询服务中心。是以“安全能力服务化，安全服务集约化”为设计原则，改变传统以特征和规则匹配为基础的产品支撑体系以及碎片化的安全服务机制的集约化安全能力输出中心。是以大数据加人工智能为驱动的智能化技术为支撑的运营管理与保障服务机制，通过汇聚相关安全数据进行协同分析，由点及面，发现安全风险的安全分析中心。是将原本零散的安全数据变成统一规范的安全数据资源为湖州市提供安全运营支撑能力的安全保障中心。是汇聚各类网络安全人才，赋能培养本地网络安全人才队伍的安全人才汇聚中心。

③运营中心是单位获取安全能力的总资源池。运营中心将整合现有安全技术保障能力、安全服务能力，让安全能力集约化、服务化、SaaS 化，形成本地化安全资源目录，对全市单位进行开放，各单位可以自主化、定制化使用安全资源能力。运营中心覆盖数字化改革基础设施安全、数据资源安全、应用支撑安全、场景应用安全建设各个维度。

④运营中心是市域一体化安全运营的总工作站。在运营层面，运营中心将统一全市电子政务安全数据归集、统一全市电子政务安全资产管理、统一电子政务安全基础策略调度、统一安全运营流程。对全市各政务外网内单位的网络、平台、数据、应用、终端等进行整体监测监管。结合浙政钉通过自动化的运营流程将安全问题通报给相关单位，并在监管机制下监督相关单位完成任务闭环。同时为单位提供安全加固与整改所需的安全技术支撑工具、安全咨询能力、安全服务等。

2. 市域一体化安全运营中心建设框架

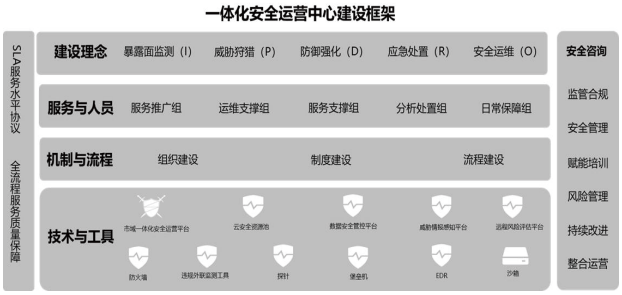

图 4 一体化安全运营中心建设框架

运营中心建设框架基于底层安全技术与工具建设，配套安全管理制度与流程，借助人员服务能力，建立 IPDRO（识别－防护－监测－响应－运营）整体安全运营体系，并对外提供安全咨询服务。

①技术与工具建设。通过各类基础设施安全防护建设构建安全能力系统，并将各种安全能力服务化，形成安全服务目录，对外提供基础安全保障能力。

②机制与流程建设。通过完善安全管理组织建设、安全管理制度建设以及配套的安全管理流程建设，构建整体的安全管理体系，实现对全市安全风险的有效管理和监督。

③服务与人员建设。构建安全运营团队，包括服务推广组、运维支撑组、服务支撑组、分析处置组和日常保障组。落地不同小组的工作职责和范围，形成联动机制。

3. 安全运营中心技术支撑平台建设

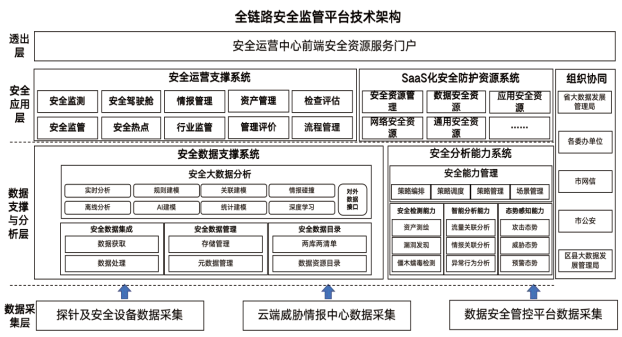

图 5 全链路安全监管平台技术架构

将由市大数据局牵头，中国电信湖州分公司全面承建全链路安全监管平台并运营，覆盖云、网、端、边界、数据、应用，结合湖州市本级、区县电子政务现网安全数据，对现网当中各类设备所产生的安全日志进行标准化梳理与整合，形成覆盖“云、网、端、数、用、边”的安全态势。同时通过公共接口服务的方式为各单位提供服务，各单位的安全设备特征库、威胁库、病毒库等相关资产也可以通过授权的方式获取公共威胁情报服务，为本地安全产品进行赋能。全链路安全监管平台与浙政钉体系打通，将湖州电子政务相关各单位的责任人、管理人员及相关角色进行有效划分，安全事件、情报、快速传达至相关单位处置。

4. 安全运营服务能力建设

①安全咨询服务。借助安全运营团队对全市各单位提供各类安全咨询服务。

②互联网应用安全服务。通过 SaaS 化应用安全监测与保障平台为各单位互联网应用提供安全防护、DDos 安全防护、内容监测、可用性监测等能力。各单位需要配合安全运营中心接入相关互联网应用系统，加强应用安全基线保障能力。

③渗透测试服务。通过真实模拟黑客使用的工具、分析方法来对业务系统进行模拟攻击，结合智能工具扫描结果和人工确认，进行深入的手工测试和分析，从而充分识别业务系统风险并要求进行整改。

④风险评估服务。通过业务调研、网络分析、安全扫描、人工检查、渗透测试等一系列服务手段全面评估信息系统的安全状况，识别安全威胁与脆弱性，分析与监管要求的差距，并要求进行整改。

⑤安全培训服务。邀请安全理论、技术专家，针对各单位数据安全业务人员和技术人员定期开展安全基础专项培训，提升相关人员安全意识，掌握数据安全发展趋势，了解新型风险和攻防新技术，规范安全管理制度，提高整体安全防护能力。建立学习激励政策，不同角度提升安全培训教育的成效，不断提升数字化改革的安全能力。相关单位应开展安全培训教育的交流和学习，分享实际工作中的安全经验，丰富安全防护的实战能力，保障数字化改革安全有效开展。

⑥代码审计服务。通过安全服务厂商提供的代码审计工具 + 人工确认 + 人工抽取代码检查的方式，根据业务流信息检查目标系统的脆弱性、缺陷以及结构上的问题，并要求进行整改。

⑦驻场运维服务。安排专业人员提供现场支撑服务，对市、区县大数据发展管理局网络安全相关的工作开展安全风险监测、策略调整和安全处置等，并定期汇报网络安全整体状况。

四、市域安全一体化建设保障措施

（一）加强组织领导

加强市域安全一体化的组织领导，构建统一领导、上下衔接、统筹有力的全市政务信息化组织体系和市、区县各单位协同联动的综合协调机制，从体制机制上消除信息共享障碍，保障建设任务的顺利推进。加强安全人员力量配备，确保市域安全一体化各项任务的有效落实。

（二）强化人才保障

营造良好的学习实践环境，加强人才队伍建设，积极引进一批科技人才和行业稀缺人才；积极鼓励和支持湖州本地高校开设物联网、云计算、网络安全等与安全运营中心建设相关的专业课程。积极培养既精通政府业务和能运用互联网技术和信息化手段开展工作的综合型人才，加快湖州市本地化网络安全人才梯队建设。

（三）创新运营模式

坚持政府引导、市场主导的原则，建立灵活边界、专业多样的安全运营机制。探索设立安全运营中心，通过购买服务的方式，承担市域安全一体化的系统建设和运维任务。扶持本地企业带方案、带技术、带团队，参与推动市域安全一体化建设。

参考文献：

[1]张杰.新时代我国市域主流意识形态网络话语权建设研究[J].三晋基层治理,2022(01):66-71.

[2]刘波,王力立.关于构建新时代网络综合治理体系的几点思考[J].国家治理,2018(38):3-7.

[3]罗进.加快构建网络安全综合防控体系服务市域社会治理的对策研究[J].武汉公安干部学院学报,2021,35(01):19-21.

[4]张继春.网络安全面临的风险挑战与战略应对[J].前线,2017(05):18-23.