# 基于 PPDR 模型的博物馆信息安全体系建设

徐秋玮

（扬州中国大运河博物馆 图书信息部，江苏 扬州 225007；扬州大学 信息工程学院，江苏 扬州 225127）

**摘要**：博物馆碎片化、加法化的传统防护体系已经难以应对持续发展的安全挑战，建设系统化、动态化、持久化的博物馆信息安全体系势在必行。通过对两个经典信息安全模型的分析，综合博物馆的属性特点，以具有较高灵活性、动态性的 PPDR 模型为基准进行讨论研究。并结合博物馆信息化管理工作实践，从策略、保护、检测、响应 4 个方面总结出适合博物馆信息安全体系建设的方法，为行业管理者提供参考。

**关键词**：信息安全体系；PPDR 模型；博物馆；信息化管理

**中图分类号**：C931.6 **文献标志码**：A **文章编号**：1671－1807(2023)03－0203－06

后疫情时代，数字化转型成为潮流，各国在各个领域对网络和信息化的依赖程度不断加深[1]。然而国际形势波诡云谲，国际关系日趋复杂，互联网成了各国博弈的新战场，信息安全成了最紧迫的威胁。由于网络空间的开放性和互通性，博物馆作为社会服务和宣传教育的前线阵地，当面临网络安全威胁时很难独善其身。

近年来，博物馆的数字化建设之路可谓充满起伏。一方面数字化的快速发展带来更大的信息安全风险，博物馆数字化的水平越高，博物馆人所要承担的“内忧”就越大；另一方面，随着国际形势的纷繁变化，信息安全已上升到国家安全的战略高度，各级政府部门和事业单位在各类项目建设的过程中也加大力度强调安全建设的重要性。信息安全管理是博物馆安全体系建设的固有组成部分，为博物馆开展研究、典藏、展览、教育、服务等工作提供重要保障。“八六三”信息安全专家组曾提出过更适合中国国情的 WPDRRC 模型，具有较强的时序性和动态性，但其主要实现对在线报税系统的安全保护，与博物馆信息安全体系难以融合。目前在中国缺少对博物馆信息安全体系的专项研究，当提及信息安全管理时很多博物馆无所适从。传统信息系统安全管理缺失，即使是新建设的信息化系统，对于如何开展安全防护工作也无处着手，专门的安全体系和模型仍处于缺失状态。为此，本文基于博物馆对业务连续性高要求的特点，通过介绍对比目前主流的动态信息安全模型，选择更符合博物馆的 PPDR 模型作为信息安全体系建设依据，从策略、保护、检测、响应 4 个角度结合管理实践论述了当今时代背景下博物馆管理者建设信息安全体系的方法，为同行业信息安全建设提供参考。

## 1 博物馆信息安全体系建设现状分析

随着大数据、云计算、人工智能、物联网等大量新兴技术的涌现，各地博物馆都在数字化、智慧化建设的路上快马加鞭，充分利用技术赋能，为博物馆注入新动力，然而一系列的信息安全问题也相伴相生。其中以系统瘫痪、页面篡改和数据泄露 3 类典型问题为主，严重影响了博物馆业务的连续性，损害了其作为大型学习教育和社会服务机构的外在形象，造成的不良影响更是在社会范围内引起广泛传播。

根据 CNCERT（国家互联网应急中心）监测统计，2022 年 2 月下旬以来，互联网遭受境外网络攻击不断，境外组织通过计算机作为跳板，对俄罗斯、乌克兰、白俄罗斯进行网络攻击。经分析，攻击源主要来自美国，仅来自纽约州的攻击地址就有 10 余个，攻击流量峰值达 36 Gbps，87％的攻击目标是俄罗斯，也有少量攻击地址来自德国、荷兰等国家[2]。这些发生在身边的安全事件刺激着博物馆对信息安全建设的投入，但由于起步晚、专项人才缺口大等原因导致仍然存在以下问题：

1）博物馆更多财力、物力投入在弱电、建筑智能化、多媒体等基础设施的安全防护上，对于其他信息和业务系统的保障能力有限。

2）目前博物馆的各个业务信息系统相互独立，

**收稿日期**：2022-09-05

**作者简介**：徐秋玮（1992－），男，江苏徐州人，扬州中国大运河博物馆图书信息部，扬州大学信息工程学院，硕士研究生，研究方向为博物馆信息化、工程管理。

导致安全保护措施较分散，存在信息壁垒。

3）博物馆一般通过一次性招投标的方式引入安全服务商，将全馆的安全规划和方案可以由一家全部承揽，缺少整体性和系统性考虑。

4）采购并部署的安全设备和软件，由于缺乏维护，导致出现应急情况时无法及时处置，长期造成资源浪费，无法有效利用。

5）博物馆员工安全意识薄弱，轻视日常检查工作，信息安全防范意识差，埋下安全隐患。

出现以上问题的根本原因是缺乏适应新形势的信息安全体系，即便有也与馆情匹配度低，缺乏长远有效的规划，缺少制度和技术保障。

## 2　信息安全体系建设的动态安全模型

安全体系的建设离不开安全模型的支撑。传统的信息安全更关注被动防御，主要通过架设防火墙、加密和访问控制来实现。随着互联网的进步，攻击源和攻击手段变得更加灵活，静态安全模型已经难以应对新的网络威胁，屏障一旦被突破，带来的危害和影响是不可弥补的。在此，就博物馆对业务高可靠性、完整性、连续性的要求，介绍两种基于时间的动态安全模型。

### 2.1　PDR 模型

PDR 模型（图 1）是保护-检测-响应（protection-detection-response）的简称，也是较早期的信息安全模型，由美国国际互联网安全系统公司（ISS）提出[3]，是体现出主动防御思想的一种网络安全模型。该模型将“承认漏洞，正视威胁，采取适度防护，加强检测，落实反应，建立威胁防护”作为指导思想，认为时间长短是衡量信息系统安全性的标准，任何安全防护措施在足够的时间内都可能被攻破[3]。

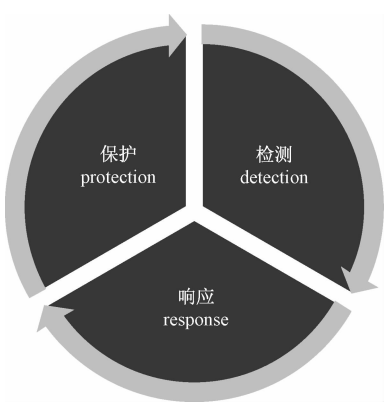


**图 1　PDR 模型**

保护（protection）就是一切可能来保护网络和系统信息安全的措施之和；检测（detection）是对网络和信息系统状态的安全检查，为保护和响应提供依据；响应（response）是解决安全问题的最有效办法，也是模型底线。解决安全问题到底还是解决紧急响应和异常处理问题，因此，对于网络和信息系统来说，建立应急响应机制，具备快速响应的能力至关重要[4]。

PDR 模型简单实用，是一个基于时间的、可证明的安全模型。简言之，信息系统的安全依赖于防护的时长大于检测与响应时间之和，即

$$P(t)>D(t)+R(t) \tag{1}$$

式中：$P(t)$为安全体系所能支撑的时间，也是系统所能防护的时间；$D(t)$为系统遭受攻击时，攻击行为被检测察觉所用的时间；$R(t)$为检测到攻击之后，系统会做出应有的响应动作的时间。

信息系统安全与否的评定标准如下：

1）$P(t)>D(t)+R(t)$，系统安全，即系统防护成功发挥了保护作用，通过有效的检测和响应抵御住了攻击和破坏行为，未给信息系统造成损失。

2）$P(t)<D(t)+R(t)$，系统不安全，即系统的保护作用未能有限发挥，在检测和响应做出之前就已经失效，攻击和破坏行为已经给信息系统造成了破坏和影响[5]。

### 2.2　PPDR 模型

PPDR 模型（图 2）是策略-保护-检测-响应（policy-protection-detection-response）模型的简称，是在 PDR 模型的基础上发展出来的模型，也称为 P2DR 模型[3]。PPDR 模型认为信息安全漏洞是不可避免的，必须基于整体安全策略指引，运用防护和检测工具来了解评估系统状态，并通过反馈响应将系统安全和风险降到最低，从而满足安全要求[6]。

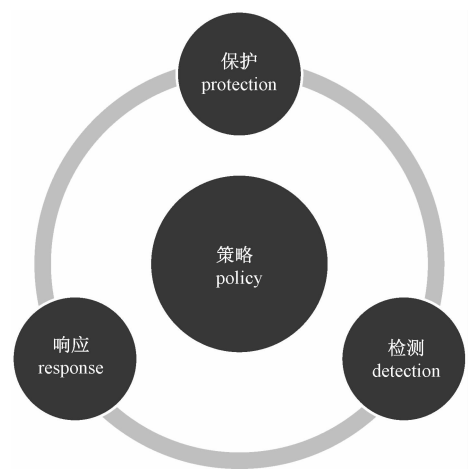


**图 2　PPDR 模型**

PPDR 模型以安全策略为核心,是动态网络安全体系的模型代表,也是动态安全模型的元老。当系统出现异常时,在安全策略的指引下迅速响应,保护系统安全。

策略(policy):模型的核心,也是所有的防护、检测和响应的依据;保护(protection):针对一切安全问题隐患和风险准备的静态安全预防措施;检测(detection):在系统被嗅探和攻击时启动,与保护构成双保险,同时为响应研判提供依据;响应(response):入侵行为直接触发事件响应与处理工作。响应包括应急响应和恢复处理,恢复处理又包括系统恢复和信息恢复[4]。

假设系统 S 的防护、检测和反应的时间分别是:$P(t)$为防护时间,即有效防御攻击的时间;$D(t)$为检测时间,即攻击开始到检测到的时间;$R(t)$为反应时间,即检测到攻击到处置结束的时间。假设系统被对手成功攻击后的时间为 $E(t)$,即暴露时间。

该系统的时间关系表达式如下:

1)如果 $P(t)>D(t)+R(t)$,那么 S 是安全的;

2)如果 $P(t)<D(t)+R(t)$,那么 $E(t)=(D(t)+R(t))-P(t)$[4]。

从上式中不难看出,当防护时间 $P(t)=0$ 时,系统的暴露时间等于检测和响应时间之和,和的值越小意味着系统越安全。由此可以得出结论:信息系统安全的关键在于防护时间的增长,检测和响应时间要尽量缩短[7]。

美国国防部在“911”恐怖事件后提出过 PDRR 模型(protection-detection-response-restore),增加了恢复环节,将信息安全事件发生后的纠错措施融入整个体系中去。中国“八六三”信息安全专家组也曾提出过新的信息安全体系建设模型WPDRRC,它在 PDRR 模型的前后增加了预警W(warning)和回击 C(counterattack)[8]。以上模型虽有创新和完善,但从最基本的原则上来说,还是围绕着 PDR 3 个核心步骤展开,尤其针对博物馆这种具有特殊影响力性质的公益性机构,更多强调的是业务持续性,运用安全策略及时发现问题,动态调整填补漏洞。

## 3 博物馆基于 PPDR 模型的信息安全体系构建

PDR 模型由于其被动性,当面对千变万化的攻击源和攻击手段时,$P(t)$、$D(t)$和 $R(t)$很难定义具体的时长,导致无法有效证明系统是否安全。相比之下,PPDR 模型则更强调防护、检测、响应和对抗的动态结合,以安全策略为导向,建立起动态循环,使得体系建设更具可控性、持续性。

以下就从 PPDR 的 4 个方面谈一谈博物馆信息安全体系构建。

### 3.1 策略(policy)

策略是 PPDR 安全模型的核心和关键,为保护、检测和响应提供方向性指导,也决定了整个安全体系的目标与强度。策略中要明确各个部分的范围和边界,明确准入行为。确立博物馆的安全策略是博物馆安全体系建设的首要工作,也是实现博物馆信息安全的第一步。

#### 3.1.1 组织管理

博物馆的员工组成较为复杂,一般分为编制与合同制。合同制的体系中根据工种和用工方式的不同还会分为若干类,导致了管理难度的增加。而信息安全体系建设强调对目标的控制,对于不同角色和职能要有清晰的管控策略。编制人员依职能划分不同的权限范围,敏感职位要给予重点关注,提高检查与考核要求。合同制人员依用工方式制定不同策略,第三方服务和驻场人员要签订保密协议,严格落实新录用和离职人员的保密责任,涉及到供应链管理的,要依据协议履行交付中的安全承诺。

#### 3.1.2 访问控制

结合组织管理结果,针对不同业务设置不同的访问控制和授权流程,防止对信息的违规篡改和滥用。基于博物馆组织结构复杂性,可建立基于角色的访问控制模型(RBAC)(图 3),职工必须成为某一角色,且当此角色被激活时,才能拥有访问和执行操作的权限。

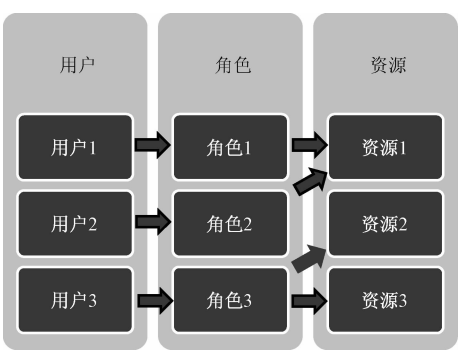


**图 3 基于角色的访问控制模型(RBAC)**

#### 3.1.3 设立安全机构

博物馆应设立专门信息安全工作领导小组或

委员会,并由信息安全工作领导小组统一负责组织指导信息安全工作。一般领导是第一责任人,部门领导作为安全主管,各部门内设安全联络人,主要负责日常安全的管理,组织信息安全培训等活动。以安全领导小组为核心,指导每年的信息安全工作规划与决策,将信息安全纳入年度重点工作,小组运营经费作为常规预算分配。

#### 3.1.4 制度保障

这里的制度保障分为两个方面:一方面是指博物馆根据行业标准和法律规范,制定适合馆情的信息安全管理制度,规范工作流程;另一方面则是将信息安全管理作为博物馆日常运营管理的一部分,比如基于已有的安全设备和防护资源建立一套巡检制度体系。运用制度指导并控制各部门作业的安全,为机房网络、终端、应用、数据等资源提供管理标准。同时,通过周期性的巡检及时发现安全隐患,为其他工作决策提供参考。

#### 3.1.5 应急预案

应急预案在日常的安全管理中体现较少,但为了保证应对突发的信息安全事件时的及时响应,尽可能地减少损失和负面影响,应急预案是信息安全管理体系中不可或缺的一部分。内容需覆盖不同种类的信息安全事件,包含联防联动体系确立,职责确认,并对处理措施与步骤有着详细的说明,具有可操作性。除此之外,应急预案每年应组织演练,提高相关人员的应急处理能力,增强信息安全意识。

以上或许超越了 PPDR 模型中对于安全策略的定义,但现阶段博物馆的信息安全体系建设若仅着眼于边界控制、授权等具体策略,显然不太全面,要为其丰富更多组织、运营和管理内涵,全方位地构建起信息安全体系。

### 3.2 保护(protection)

保护是整个 PPDR 模型中最为关键的一环,拥有可靠的保护措施会使得整个体系建设变得简单省力,如果保护做得好,入侵攻击行为被挡在门外,那么检测的压力就会减轻;反之,检测的责任就越大。受到组织环境和资源条件的限制,博物馆在实际部署保护措施时各不相同,但不能否认在建设信息安全体系这一目标上的一致性。

#### 3.2.1 网络机房保护

博物馆信息化、数字化建设离不开网络机房的支持,但建设规模上不尽相同。有的会建设主机房和分机房,有的可能只是按区域或楼层划分建设。但不论何种,对机房的保护是相同的。首先,机房的温度、湿度和除尘是基本;其次,切忌储藏杂物,确保环境的安全卫生;再次,天花板和地板的防水防潮处理,机房内的消防设备检查等是对安全的进一步巩固;最后,在策略的指导下,要对机房进出人员的管控保持敏感,尤其在重点时段和恶劣天气时段更要提高警惕。

#### 3.2.2 终端设备保护

在博物馆中终端设备分为两类,一类是办公区的电脑,另一类则是展览区的显示屏、公共广播、数字多媒体以及物联网设备。办公区的电脑集中与互联网交互,要对钓鱼、病毒入侵等行为提高警惕,每个部门设立的安全联络员要定期巡查,敏感数据应使用独立且脱机的设备处理与存放;展览区的设备统一管理,要严格控制与互联网的连接,做到非必要不联网。有远程连接需求的,可以考虑开放定向加密端口或者 VPN 方式来实现。

#### 3.2.3 软件保护

对软件的正版要求在博物馆管理中不仅是防止侵权,更多在于对盗版软件留有后门的安全防范。其中除了涉及常用的操作系统、办公、绘图系列软件,杀毒防护软件也是不可缺少的一部分。这里的杀毒软件不仅是针对办公电脑,还包括服务器主机等安装有独立操作系统的终端设备。此外,远程控制软件也存在安全隐患,为外来入侵提供可乘之机,要警惕远程控制软件的威胁。随着国家信息安全战略调整,系统和软件的国产化替代在博物馆范围内也应该引起重视,把安全牢牢掌握在自己手中。

#### 3.2.4 防火墙保护

防火墙自 20 世纪 90 年代问世以来已经发生了若干代的革新,对于博物馆比较常见的一般有网络防火墙、应用防火墙还有云时代应运而生的云防火墙。网络防火墙是架设在内外网之间的一道安全屏障,实现逻辑分离。当然这里也要提到关于内网中的物理隔离、VLAN 划分和静态 ARP 绑定等措施,某种意义上都是从网络层进行了分隔,保证了业务间的通信管控,这对于任何建设有机房或弱电间的博物馆来说都是基础的安全保障。应用防火墙比较常见的是用于博物馆网站的 WAF(网站应用级入侵防御系统),它是通过一系列的策略配置来进行入侵防御、访问控制、审计监控等防护。而云防火墙有效利用了云时代的特点,运用多节点、CDN 加速、数据共享等手段对博物馆网站等暴露在公网的 web 应用提供防攻击、防篡改、防瘫痪、防泄露等防护,但云防火墙与 web 应用的兼容性各不相

同,具体还需结合情况进行测试。

#### 3.2.5 冗余备份保护

在分布式架构盛行的今天,冗余备份可能不再被认为是资源的过度投入,这种思想对于博物馆来讲尤为重要。对于保障业务连续性的关键设备和系统都应采取冗余备份策略,包括网络防火墙、业务系统服务器、数据存储阵列等。它不仅对资产起到保障作用,更是为应急事件发生后的处理提供了有效支撑。

#### 3.2.6 日志审计保护

日志审计现多作为问题发生后的溯源手段之一,可以有效排查问题的起因经过,推断出问题的根源所在。2017 年 6 月 1 日起施行的《中华人民共和国网络安全法》中规定:采取监测、记录网络运行状态、网络安全事件的技术措施日志应保证不少于 6 个月的留存,等级保护中也对日志的留存提出了要求。日志审计可以为博物馆信息系统提供分析依据,帮助管理者获悉系统状态,及时识别内外部的安全隐患。

#### 3.2.7 密码保护

密码在信息系统的身份鉴别、访问控制和审计中发挥重要作用,同时也是入侵者打开大门的钥匙。当入侵者发起漏洞攻击受阻时,往往就会从密码下手寻找逻辑漏洞,进行暴力破解。这就要求博物馆信息管理者在设置账号密码、平台密码、端口加密、数字证书时要符合保密等级要求,尽量使用复合型无序密码,启用密码定期更换和冻结机制。另外根据等保要求要定期参与密码应用安全性评估,保证密码侧无机可乘。

#### 3.2.8 社会工程学保护

社会工程学真正作为学科出现是在 20 世纪 60 年代,是指通过与他人交流,使其心理受到影响,做出某些动作或者是透露一些机密信息。这通常被认为是以欺骗他人来获取所需信息行为[9]。简言之,通过交流套取机密信息,对被害人进行定位,从而进一步对目标进行渗透攻击。博物馆中人群构成较为复杂,有些馆对于办公区和游客区的划分不是很清晰,经常出现游客误入。如果有人伪装身份进入办公区进行信息搜集,会导致不可想象的后果。除了制度约束外,要将安全教育纳入年度工作计划,提高全员安全意识,杜绝一切主动与被动的信息泄露,养成随手关门、人走锁门、废弃材料不出门的好习惯。

### 3.3 检测(detection)

检测在 PPDR 模型中起到第二道屏障的作用。在策略和保护的基础上,检测可以在安全问题发生之前有效识别风险,检查自身的脆弱性,防微杜渐。

#### 3.3.1 等级保护测评

自 2017 年 6 月《网络安全法》出台后,等级保护测评正式立法。等级保护从 1.0 时代进入到 2.0 时代后,范围和标准也有所提高。如果系统是关键基础设施(即被入侵后可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等),还需要在等保的基础上做重点保护。

对于博物馆系统而言,常见的等保定级在二级和三级。比如偏向展示宣传类的门户网站、新闻平台等非交互性系统一般为二级等保,根据相关要求每两年做一测评备案;但是票务、观众预约等涉及个人隐私,与身份证、社保卡等跨平台对接的交互性系统,一般定为三级,根据相关要求每年需完成一次测评备案。等保测评会对系统的软硬件安全防护措施进行全面评估,如果测评出现问题要接受安全整改。可见,等保测评对于博物馆来说既是责任,也是法定义务。

#### 3.3.2 漏洞扫描

漏洞扫描是一项基础而重要的信息安全技术,它与防火墙配合能够有效提供业务系统安全性。其主要基于漏洞数据库,对指定的计算机或业务系统进行脆弱性检测,通过数据比对发现可利用漏洞,也是为进一步的渗透测试提供依据。漏洞来源于不规范的代码编写、网络协议、操作系统等,即便某个阶段消除了所有已发现漏洞,随着系统和软件的更新,也会有新的漏洞产生。对于博物馆来说,保证对业务系统的周期性检查是很有必要的。目前互联网上也有很多开源的漏扫工具,但需要一定技术基础来操作使用,而漏扫设备的价格又参差不齐,每个博物馆的承载能力也有限,可以考虑购买服务的方式为业务系统开展基本的“体检”。

#### 3.3.3 渗透测试

渗透测试可以理解为在扫描到漏洞的基础上,进行二次验证而发起的攻击。其定义没有统一规定,一些安全组织称其为通过模拟入侵者攻击从而来评估系统安全性的一种方法。这个方法包括任何可能的漏洞利用与分析,也包括任何有利的攻击源,渗透的深度也取决于攻击者的技能水平。渗透测试会将渗透情况形成报告,对入侵的过程和细节做出具体描述,明确指出安全威胁。配合漏洞扫描,博物馆可以适当降低渗透测试的频次,但要确保每年至少 1~2 次。这可以协助管理者优化安全策略,排除安全风险。即使渗透测试未能成功攻

破，也可以证明现有的防护措施是安全有效的。

#### 3.3.4 威胁感知

事实上，对于威胁感知，防火墙等防护措施中已经集成。通过对威胁感知和告警规则的设置，可进行对入侵行为的实时监控。针对更深层次的数据安全感知，也有入侵检测系统（IDS）和入侵防御系统（IPS）的支持，及时感知发现各种攻击企图、攻击行为或者攻击结果，并记录及报警。博物馆信息管理者需具备威胁感知的基本能力，对高频次、有目的性的攻击行为进行 IP 管控，同时结合自身情况，借助软、硬件防护手段并行监控，在威胁入侵之后、损失发生之前及时发现。

### 3.4 响应(response)

响应在 PPDR 模型中是最后一道防线，也是底线。在策略的基础上，要积极提高安全队伍的业务水平和应急响应能力，按照发现事件、先期处置、事件报告、应急处置、恢复重建、总结评估的流程定期组织演练，动态调整响应队伍，形成良好的沟通与合作机制。

#### 3.4.1 开展攻防演练

根据要求，网信和公安部门每年会组织攻防演练等护网行动，博物馆作为直属或下级单位要积极参加。一方面将业务系统交给专业工程师众测，发现问题；另一方面当遭遇入侵攻破时，锻炼队伍的风险研判和安全处置能力，积累应急响应经验，提升安全防护能力。

#### 3.4.2 组织培训和竞赛

面向博物馆工作人员，组织安全意识教育和安全实操能力培训。内容涵盖安全领域的多个方面，通过安全专题培训学习和配套的教学实验，提升信息安全领导小组专业化工作水平，增强普通员工的信息安全意识，保障信息安全体系稳定运行。培训结束后可通过组织竞赛方式考评，既能检验培训成果，又能调动全员参与的积极性。

## 4 结语

博物馆的信息安全体系建设不是简单的软、硬件堆叠，而需要立足馆情，从实际出发，处理好数字化博物馆建设与信息安全的关系。PPDR 模型中的动态防护思想为新阶段博物馆构建信息安全防护体系提供了参考。博物馆人要树立正确的安全观，人防与技防相结合，让安全防护的“事前、事中、事后”连成一条线，不断优化体系建设内容，全面考虑建设过程中各个环节的协同机制，形成 PDCA 的良性循环。处理好“内忧”，对抗住“外患”，莫让信息安全的木桶出现“短板”。

## 参考文献


[1] 杨晓强，李若瀚. 国际网络空间安全治理：困境、反思与对策[J]. 河南社会科学，2022，30(6)：101-109.

[2] 国家互联网应急中心[EB/OL]. [2022-03-11]. https://www.cert.org.cn/publish/main/49/2022/20220311143503444781001/20220311143503444781001_.html.

[3] 蔡利军，周益飞. 从 PPDR 模型看高校信息安全保障工作[J]. 中国教育网络，2018(10)：70-72.

[4] 网络信息安全之基于时间的安全模型(PDR 和 PPDR 模型)_xiejava1018 的博客-CSDN 博客[EB/OL]. (2022-04-26) https://xiejava.blog.csdn.net/article/details/124359142.

[5] 网络安全教程(3)_予我心安 A3 的博客-CSDN 博客[EB/OL]. [2022-03-23]. https://blog.csdn.net/yuwoxinanA3/article/details/123557996.

[6] 常见的网络安全模型_七天啊的博客-CSDN 博客[EB/OL]. [2022-03-22]. https://blog.csdn.net/sycamorelg/article/details/123430405.

[7] 黄勇. 基于 P2DR 安全模型的某银行信息安全系统方案设计[D]. 合肥：合肥工业大学，2010.

[8] 李尧. 从 PDR 模型的发展过程看信息安全管理[J]. 电子产品可靠性与环境试验，2012，30(4)：35-37.

[9] 金涛，吴晓文. 基于社会工程学网络渗透方法的研究[J]. 网络空间安全，2021，12(S2)：57-62.


## The Construction of Museum Information Security System Based on PPDR Model


XU Qiuwei

(Library and Information Department, China Grand Canal Museum, Yangzhou Jiangsu 225007, China;
College of Information Engineering, Yangzhou University, Yangzhou Jiangsu 225127, China)



**Abstract**: It is difficult for the traditional protection system of museum fragmentation and addition to meet the security challenges of sustainable development. So, it is imperative to build a systematic, dynamic and lasting museum information security system. Based on the analysis of two classical information security models and the characteristics of the museum, PPDR model has higher flexibility and dynamics. Combined with the practice of museum information management, the methods suitable for the construction of museum information security system are summarized from four aspects of strategy, protection, detection and response, so as to provide reference for information managers of same industry.



**Keywords**: information security system; PPDR model; museum; information management