

# 谈电子档案信息安全评价指标体系的构成

**摘要** 电子档案信息系统是一个复杂的系统工程。文章从物理安全评价指标、管理安全评价指标、网络安全评价指标、信息安全评价指标、系统安全评价指标5个方面,阐述了电子档案信息安全评价指标体系的构成。

**关键词** 电子档案 信息安全 评价体系 构成

◇王娜

电子档案信息系统是一个复杂的系统工程,既有硬件,又有软件,既有外部影响,又有内部因素,而且许多方面是相互制约的。因此,必须要有一个规范的、统一的、客观的标准。根据国内外的电子档案信息安全评估标准,以及国家对电子档案信息和网络信息系统安全性的基本要求,结合电子档案管理和网络管理经验,综合考虑影响电子档案信息安全的各种因素,笔者认为,电子档案信息安全评价指标体系的构成应包括如下内容:

## 1. 物理安全评价指标

物理安全是指存储档案信息的库房、计算机设备和管理人员工作场所内外的环境条件必须满足档案信息安全、计算机设备和管理人员的要求。对于各种灾害、故障要采取充分的预防措施,一旦发生灾害或故障,能采取应急措施,将损失降到最低。物理安全包括环境安全、设备安全和载体安全三个方面:(1)环境安全:主要指存储档案信息的库房、计算机机房周围环境是否符合管理要求和是否具备抵抗自然灾害的能力,如库房是否建在电力、水源充足、自然环境清洁、通讯、交通运输方便的地方;有无防火、防水措施;有无监控系统;有无防雷措施等。(2)设备安全:主要是指对电子档案信息系统设备的安全保护,包括防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等。(3)载体安全:要对载体采取物理上的防盗、防毁、防霉等措施。

## 2. 管理安全评价指标

安全管理在电子档案信息安全保障中起着规范和制约的作用,科学的管理理念加上严格的管理制度才能最终保证电子档案信息的安全。电子档案信息的管理安全评价指标具体包括:(1)专门的档案信息安全组织机构和专职的档案信息安全管理:档案信息安全组织机构的成立与档案信息安全管理人员的任命必须有相关单位的正式文件。(2)规章制度:包括有无健全的电子档案信息安全管理规章制度;档案信息安全人员的配备、调离是否有严格的管理制度;设备与数据管理制度是否完备;是否有登记建档制度;是否有完整的电子档案信息安全培训计划和培训制度;各类人员的安全职责是否明确,能否保障电子档案信息的安全管理。(3)是否有紧急事故处理预案:为减少电子档案信息系统故障的影响,尽快恢复系统,应制定故障的应急措施和恢复规程以及自然灾害发生时的应急预案,制成手册,以备及时恢复系统运行。

## 3. 网络安全评价指标

越来越多的电子档案在网络上传输,而网络作为一种构建在开放性技术协议基础上的信息流通渠道,它的防卫能力和抗攻击能力较弱,可能会遭受到病毒、黑客的袭击。为了保证电子档案的安全,必须保证其传输的媒介——网络的安全,网络安全评价指标包括以下几个方面:(1)是否有计算机病毒防范措施。(2)是否有黑客入侵防范设施:主要是设置防火墙和入侵检测等设施。(3)是否有访问控制措施:访问控制是指控制访问网络信息系统的用户,当用户之间建立链接时,为了防止非法链接或被欺骗,就可实施身份确认,以确保只有合法身份的用户才能与之建立链接。(4)是否有审计与监控设备:审计与监控是指应使用网络监控设备

或实时入侵检测设备,以便对进出各级局域网的常见操作进行实时检查、监控、报警和阻断,从而防止针对网络的攻击与犯罪行为。

## 4. 信息安全评价指标

在网络能够正常运行的基础上,我们要保证在系统中传输、存贮的电子档案信息是安全的,不被截取、篡改或盗用。(1)是否采取加密措施:档案的本质属性是原始记录性,而计算机和网络的不稳定性使得电子档案信息的安全性难以保证,而且有些电子档案信息有密级限制,不能公开在网络上传输,所以电子档案信息在网络传输时必须通过加密来保证其安全。(2)是否有数据完整性鉴别技术:网络传输使得电子档案信息的完整性无法保证,黑客的攻击可以改变信息包内部的内容,所以应采取有效的措施来进行完整性控制。(3)是否确保信息数据库的安全:一个组织最核心的信息通常以数据库的形式保存和使用,保证数据库安全对于电子档案信息来说有重要的作用。(4)是否有信息防泄漏措施:信息防泄漏包括信息审计系统和密级控制两方面。信息审计系统能实时对进出内部网络的信息进行内容审计,以防止或追查可能的泄密行为;密级控制可根据信息保密级别的高低划分公开范围,并对用户划分访问权限,进行分组管理。(5)是否有防抵赖技术:防抵赖技术确保用户不能否认自己所做的行为,同时提供公证的手段来解决可能出现的争议,它包括对数据源和目的地双方的证明,常用方法是数字签名。

## 5. 系统安全评价指标

系统安全是指计算机整个运行体系的安全。在计算机上处理信息时,硬件、软件出现故障或误操作、突然断电等都会使正在处理的信息丢失,造成无法弥补的损失。我们需要采取一系列措施保证系统的稳定,确保信息的安全。计算机系统安全评价指标有:(1)是否有系统操作日志:系统操作日志详细记录了系统的操作状况,以便事后分析和追查系统损坏的原因,为系统提供进一步的安全保障。(2)是否进行系统安全检测:运用系统安全检测工具对计算机和网络进行安全检测,可及时发现系统中存在的漏洞或恶意的攻击,进而采取有效的补救措施和安全策略,达到增强网络安全性的目的。(3)是否有操作系统防破坏措施:操作系统集中管理系统的资源,是计算机系统赖以正常运转的中枢,它的安全性将直接影响到整个计算机系统的安全。操作系统应当建立某些相对的鉴别标准,保护操作系统本身在内的各个用户,阻止有害功能的运行。(4)是否进行系统信息备份:日常备份制度是系统备份方案的具体实施细则,应严格按照制度进行日常备份,否则将无法达到备份方案的目标。(5)是否有灾难恢复系统:当系统因人为或自然因素受到破坏时,我们应保证能够尽快地恢复正常工作,把损失控制在最小范围内。

## 参考文献

1. 魏倩. 基于模糊层次分析法的网络信息安全评价研究. 长春: 吉林大学, 2008
2. 郭振民, 胡学龙, 姜会亮. 网络与信息系统安全性评估及其指标体系的研究. 现代电子技术, 2003.9

[责编 赵晶莹]