目　录

第一章 导　言

1.1 研究背景

近年来，随着档案信息化建设的不断发展，电子文件与电子档案信息积累越来越丰富，其服务国计民生的作用也日益凸显。社会对电子文件与电子档案信息的共享利用要求也越来越高，公众希望档案部门能够提供更方便快捷的利用方式。信息化和网络技术的发展不仅仅带给公众更方便快捷的档案利用体验，同时也带来一系列与传统的档案安全不同的安全问题。近年来，针对我国互联网站的篡改、后门攻击事件数量，呈现逐年上升的趋势，尤其是政府网站已成为重要的被攻击目标。根据国家互联网应急中心发布的《2015 年中国互联网网络安全报告》，2015 年发现网络安全事件超过 12 万起，同比增长 125.9%。

档案行业历来对于信息的安全有较高的要求。档案信息是一类特殊而重要的信息资源，具有“存凭、留史、资政、育人”等不可替代的作用。随着档案信息化建设的不断发展，为应对大数据时代的机遇与挑战，各级国家综合档案馆正积极稳步推进数字档案馆建设。在数字档案馆建设极大丰富馆藏档案信息资源的同时，也对档案信息的安全保存和长期可用提出了挑战。

我国的档案利用工作开展较早，1954 年《宪法》颁布后就赋予了全体人民利用档案的权利。随着信息化时代的到来，档案信息利用服务更加系统性，由封闭型走向开放型，同时利用的方式也更加多样

化、主动化，利用的群体也越来越复杂。尤其是信息时代的到来，使得社会公众很方便地就可以在网上获取到各类档案信息，这也使得档案信息利用过程中的安全形势更加严峻。由于电子文件与电子档案的特性，从其形成之时，在传输、保存和利用等环节就受到各方面因素的影响，如电子文件易于复制、易于修改、易损、非直接可读、形式与内容容易分离等特性，以及各种外在因素如病毒和黑客攻击，各种误操作等。作为国家信息资源重要组成部分的档案信息资源，一旦泄漏、丢失和被篡改，有可能造成重大的政治和社会影响。各级国家综合档案馆是各类电子档案的永久保管基地，在电子档案信息共享利用过程中，如何确保档案信息的安全，已成为各级国家综合档案馆所面临的新课题。

随着国际上出现多起信息泄密事件后，电子文件与电子档案信息的安全管理也备受关注。2009 年 12 月 8 日，中共中央办公厅、国务院办公厅印发了《电子文件管理暂行办法》，组建了由中共中央办公厅牵头，国务院办公厅、国家发展和改革委员会等 8 个部委参加的国家电子文件管理部际联席会议，正式将电子文件管理纳入国家战略。在《办法》中，把安全保密和统一管理、全程管理、规范标准、便于利用等并列为电子文件管理的五大基本原则，并提出按照国家信息安全等级保护标准和涉密信息系统分级保护管理规定建立电子文件管理系统和信息内容安全保密防护体系，执行严格的安全保密管理制度；按照国家有关法律法规和规范标准的要求，采取有效技术手段和管理措施，确保电子文件信息安全。

2010 年 5 月 21 日，时任国家档案局局长杨冬权同志在全国档案安全体系建设工作会上的讲话强调档案安全的重要性，档案安全体系的建设需要解决公共档案信息服务与档案信息安全之间矛盾，并提出要加强电子文件的安全保护技术研究。2013 年 7 月，为贯彻落实国家信息安全等级保护制度，国家档案局结合档案行业实际，颁布了《档案信息系统安全等级保护定级工作指南》，以指导档案信息系统安全等级保护的定级工作，提高档案信息系统的安全防护能力和水平。2016 年 1 月，为指导和规范档案部门进一步加强档案信息系统建设和管理，国家档案局印发了《档案信息系统安全保护基本要求》，从管理和技术两方面，详细地描述了在档案行业实施信息系统安全等级保护的要求。2016 年 4 月，为全面贯彻习近平总书记、李克强总理关于加强安全生产工作的重要指示批示精神，深入推进档案安全体系建设，国家档案局印发了《关于进一步加强档案安全工作的意见》，就进一步加强档案安全工作提出要求。特别是在档案信息管理风险治理方面，《意见》强调，各部门各单位要在环境及设备安全、网络安全、系统安全、数据安全和数据载体安全等方面制定完善信息安全策略并贯彻执行。由此可见国家在档案信息安全方面的重视程度。

在档案信息安全领域，各级国家综合档案馆对档案信息的管理涉及到电子档案生命周期中的“收、管、存、用”等过程。其中，尤其需要引起重视的是档案信息的利用过程，它是利用体系和安全体系的结合点，也是整个安全体系的薄弱环节。在各个过程中，利用过程中的安全隐患最大，既容易在过程中遭到主动的攻击和窃取，如黑客、

病毒、木马的攻击，非授权的访问，故意的窃取、篡改和伪造等；也可能由于缺乏相应的管理、预防导致被动式的数据丢失、损坏等，特别是在电子环境下，其安全问题更加复杂化。

档案信息在利用过程中的安全保护如此重要，除了加强档案部门内部管理、控制及规范工作流程外，还需要对电子文件与电子档案管理系统进行安全保护功能的设计与实现，用技术手段保护档案信息的安全，防止档案信息经由各种非正常渠道外泄，特别要关注在档案信息动态利用过程中的安全问题。然而，从国内的现状来看，对于电子文件与电子档案管理系统相关的安全功能与技术实现，主要还是侧重于实现文档防泄密的单一静态管理功能，体现在实现文档管理、透明加密、数据备份等方面，还没有考虑在动态利用过程中主动式的安全保护。

国内对电子档案利用过程中安全的解决方案，还主要停留在防火墙、入侵检测、网络防病毒等被动防护手段上。据统计，2012 年，全球 98.2%的计算机用户使用杀毒软件，90.7%设有防火墙，75.1%使用反间谍程序软件，但却有 83.7%的用户遭遇过至少一次病毒、蠕虫或者木马的攻击，79.5%遭遇过至少一次间谍程序攻击事件。同时，据调查显示，互联网接入单位由于内部重要机密通过网络泄密而造成重大损失的事件中，只有 1%是被黑客窃取造成的，而 97%都是由于内部员工有意或者无意之间泄露而造成的。当前，档案部门对电子文件与电子档案管理系统在利用过程中的安全保护问题缺乏应有的重视，主要表现在：一是对离开业务系统后数据的利用安全考虑较少，这就

导致了在加以授权访问控制情况下，仍有信息泄密的情况发生；二是由于电子档案数据与纸质数据相比有着不同的特性，从快速流转到易于存储，从多媒体编辑到远程调阅，电子档案数据既表现出了不可替代的优越性，也使得存在的风险大大增加。在电子档案利用的全过程中，每个环节都可能存在档案被调用、查看的操作，由于电子档案的易复制和难控制使得电子档案的调阅可能出现“一人借阅、众人共享”、“一次调阅、终身使用” 等情况，也容易被窃取和篡改，导致数据的外流和档案信息的泄密。

因此，对于电子文件与电子档案而言，不仅要关注系统与数据的日常管理过程中的保护，更重要的是要解决这些系统与数据在动态的利用过程中的信息安全保护问题。目前国内缺乏相关的研究，主要表现在以下几个方面：

1. 缺乏针对档案信息利用过程的研究。大部分的研究参照一般信息安全的架构，从物理、网络、应用、数据等层面讨论信息安全，较为宽泛，尤其是由于无法结合档案信息利用过程和应用场景，因此解决方案缺乏针对性，无法有效解决安全隐患。

2. 没有突出在安全保护过程中的主动性。大部分的电子文件与电子档案管理系统采用被动的防御体系，无法对各类行为作出有效的判断，从而采取动态的防御措施，尤其对系统内部的人员操作往往无法管控到。

3. 缺乏系统性探讨实现方式的研究。大部分的研究一般只是介绍相关技术以及该技术的应用，或针对电子档案生命周期的某个环

节，缺少从利用过程中的信息安全保护需求出发，整体设计实现方式，因此系统性不足。

正是因为看到了以上的问题，本课题专门针对我国在档案信息利用过程中安全保护研究的空缺而提出，以期通过课题的研究，梳理电子档案信息在利用过程中安全保护的现状，以及存在的风险，进而提出相应的系统功能需求及实现方式，构建一个主动性、动态性、全过程的档案信息利用过程安全保护体系。课题成果将丰富我国信息安全类保护体系研究，对推动我国电子政务、档案信息化发展以及档案信息利用工作具有一定的作用。

1.2 基本概念

1.2.1 档案信息

档案是社会、政治、经济、文化、生态等各方面活动的真实记录，是社会各界察往知来的原始凭证。档案信息是指档案中反映事物特征、运动状态、方式及规律的，已经过加工处理有序化并能够提供利用的数据的集合。

由此可见，档案信息的概念从属于信息领域，是一类特殊而重要的信息，是国家信息资源的重要组织部分。与一般信息相比，除了一般信息可分享性、可扩散性、可浓缩性、可处理性的属性外，档案信息还具有原始性、凭证性、回溯性、社会性等特点。

本课题所称的档案信息，既包括数字档案本身，如数字化加工生成的档案原文、原生电子档案等，也包括各类档案的相关信息，如档

案目录信息，元数据信息等。

1.2.2 档案信息利用

档案信息利用是档案工作的重要组成部分，是档案工作的最终目的。在档案的各项业务中，档案的利用是根本所在。

本课题所指的档案信息利用，是指为了某种需要或特定目的，将档案信息应用于实践活动，以实现预定目标，使档案信息价值得以实现的过程。档案信息利用是档案信息生成、开发过程的延续，它包含着利用者这一主体的参与，最终为个人和组织提供信息支持。

1.2.3 电子文件与电子档案管理系统

本课题所指的电子文件与电子档案管理系统，泛指在电子文件与电子档案在各级国家综合档案馆内“收集、管理、存储、利用”整个过程中涉及的信息管理系统。它的定义是：“提供电子文件或电子档案各项管理功能的系统的统称。”

电子文件与电子档案管理系统承载着各类档案信息，同时也对档案用户的操作进行着管控，它的安全保护功能的设计与实现，与档案信息的安全息息相关，如果设计不当，即使有防火墙、入侵检测等安全设备，仍然会对档案信息安全造成很大的威胁。可以说，管理系统的安全是档案信息安全的最后一道保障，也是最为重要的一道。尤其是在档案信息利用过程中，系统要与外界进行交互，既涉及到内部管

理人员，更涉及到外部形形色色的利用者，因此其功能需求与实现方式更应当关注。

1.3 研究内容

本课题旨在研究和明确各级国家综合档案馆电子文件与电子档案管理系统在档案信息利用过程中的安全风险和安全保护功能需求，系统规划设计针对需求现状的主动性、动态性、全过程的利用过程中的档案信息安全保护系统的技术实现方式及其管理体系，为各级国家综合档案馆利用过程中的档案信息安全保护工作提供一个切实可行的技术解决方案和方法指导。

1．梳理档案信息利用安全保护需求

结合档案应用场景，对档案信息利用安全现状和各个相关环节的安全风险点的分析，梳理出各级国家综合档案馆电子文件与电子档案管理系统在档案信息利用过程中的安全保护需求，为安全保护功能的设计提供依据。

2．系统设计档案信息利用安全保护功能

结合现有的安全技术手段，从安全现状和需求出发，依据档案信息安全保护相关理论，确立档案信息利用安全保护的原则和目标，系统设计电子文件与电子档案管理系统在档案信息利用过程中的安全保护功能，提出具体的、切实可行的实现方式。

3．探讨档案信息利用安全保护体系

以切实保障利用过程中的档案信息安全为主线，结合功能设计和

管理手段，为档案信息利用的安全保护提供一种全新的解决思路，从组织规划、制度规范、日常管理、人才队伍、应急预案等方面入手，为建立更加全面、合理、实用和先进的档案信息利用安全保护体系提供参考。

1.4 研究意义

信息技术在档案部门的广泛应用，一方面为档案管理和利用提供了高效便捷的手段和方法，另一方面也给档案信息安全带来了新的隐患，档案信息安全问题日益突出。在数字档案馆“收、管、存、用”四大业务流程中，尤其在利用过程中，由于对档案信息的操作类型复杂，涉及各种门类的档案信息和各种各样的利用者，有可能对档案信息造成破坏,有可能导致档案信息非授权的访问、传播，因此带来了更多的风险点。课题研究将结合各级国家综合档案馆的电子文件与电子档案管理系统，实现档案信息的安全保护，使得对业务系统内信息和源于系统后来又脱离系统的档案信息的操作完全在可控范围内完成，从而保证信息不被泄露和免遭破坏。课题研究采用文件生命周期管理和风险管理的理念，建立主动性、动态性、全过程的安全防护体系，实现电子文件与电子档案安全利用管理的要求，将为电子文件生命周期的安全管理奠定基础，进一步提升电子文件与电子档案安全管理水平，同时，通过建立有效的安全保护模式来促进档案信息的共享利用，充分发挥档案信息的社会效益和经济效益。具体的意义有以下几个方面：

1．促进档案信息的有效利用。前面提到档案信息的利用价值，但由于档案信息对软硬件设备的依赖性，易逝和易变性，对背景信息和元数据的依赖性等，尤其是档案信息在利用过程中具有动态性的特点，使得其易被破坏或篡改，而且一旦遭到破坏或篡改，造成的损失往往难以弥补。档案信息还存在着易复制易传播的特点，对于它的防窃取、防泄密的工作也要加强。由于这些因素，影响了其利用价值的有效发挥。课题研究综合运用风险管理理论和文件生命周期理论，结合利用过程中的应用场景，全方位、多角度考虑档案信息在利用中可能遇到的安全风险，分析其功能需求，对适用于利用过程中档案信息安全的技术手段进行分析，提出建立主动性、动态性、全过程的利用过程中档案信息安全保护系统及其管理体系，为各级国家综合档案馆进行利用过程中的档案信息安全保护提供解决方案和方法指导，确保档案信息的安全，保护档案信息的价值和版权，为充分发挥档案信息的社会效益和经济效益提供安全保障。

2．为建设安全可靠的电子文件与电子档案管理系统提供参考。电子文件与电子档案管理系统已在许多档案部门开始建设，许多地方已初现雏形，但是在系统安全方面的考虑却没有与时俱进，与传统的馆藏档案管理系统没有太大不同，没有充分针对档案信息的特性。课题研究针对档案信息利用过程，系统提出电子文件与电子档案管理系统在档案信息利用过程中安全保护功能需求与实现方式，采用主动性、动态性、全过程的安全保护策略，充分与原有的安全体系相结合，对于各级国家综合档案馆进行电子文件与电子档案管理系统或数字

档案案管理系统建设时提升系统的安全防护水平，完善系统的功能，有着积极的参考价值。

3．推动档案信息安全体系建设。近年来，档案信息安全越来越受到重视，目前的安全保护体系还有一定的提升空间。课题研究提出建立事前、事中、事后的立体防御，结合基本安全防护和各流程动态安全保护于一体，弥补了档案信息安全保护研究之不足，对于形成成熟的档案信息安全保护机制，完善档案馆的电子档案信息保护体系具有一定的价值。课题研究结合技术和管理手段，为今后各级国家综合档案馆管理系统在档案信息利用等管理过程中的安全保护提供指导，为建立更加全面的、合理的、实用的和先进的档案信息利用安全保护体系提供参考。

第二章 档案信息利用安全保护现状及风险分析

2.1 国外档案信息安全保护情况概述

国外对于档案信息安全的关注比较早，在采取具体措施方面也就着手的比较早。国外对于档案信息的保护，一方面是完善相关法律、法规，为档案信息的保护提供法律依据;另一方面是展开对档案信息安全的研究，有效保障档案信息的安全。通过学习国外的先进经验，可以为我们进行档案信息利用安全提供相应的指导。

在档案信息安全保护方面，加拿大和美国是两个值得我们关注的国家。两国政府和研究机构对档案信息安全问题高度重视，在开展相关研究的同时，制订了一系列的相关法律、法规，为档案信息安全工作提供了较为全面的保障。

（1）加拿大在《档案信息获取法》中规定了公民在获取档案信息方面的权利;与此同时，在这部法律中规定设置“档案信息专员”这一职位，其工作职责是协助法院处理与档案信息有关的一些法律纠纷。在任命程序上，档案信息专员要经过议会的任命才能够正式履职，在级别上与副部长同级。与《档案信息获取法》相配套的《个人隐私法》，这部法律的立法宗旨就是要确保个人档案信息在披露以及公开方面的安全，避免通过滥用个人信息侵犯他人的合法权益。同时，加拿大还制定了《数据库保护法》、《计算机犯罪法》、《计算机安全监管法》等一系列的配套法律法规。通过这些法律、法规，为加拿大

档案信息安全保障工作构建了完善的法律、法规体系，在法律层面上保障了档案信息的安全。

加拿大政府充分认识到，除了在法律、管理制度方面加强对档案信息安全的保护之外，还应当从技术方面加强对于档案信息安全的保护。在技术方面加强对于档案信息安全的保护，主要从三方面来着手：

一是要加强对于档案信息的加密。对档案信息进行加密，是加强对档案信息安全保障的最基本也是最核心的技术措施。早在 1995 年，加拿大政府就授予了自然科学和能源委员会、医学研究委员会、社会科学与人文科学研究委员会三个委员会开展对于档案信息安全保护研究的权利。二是档案信息的确认技术。档案信息的确认技术，是指通过严格的限定信息的共享范围，防止档案信息安全被侵害。在这一方面，加拿大政府认为，一方面每一个人都有获得档案信息的自由，每一个家庭也都应当充分地享受到档案信息服务；在另一方面，个人权利的滥用很可能会造成对他人利益以及公共利益的侵犯，因此，应当设置安全的信息确认方案。这些信息确认方案应当达到合法的接收者能够通过一些途径来验证其所得的信息是否真实的效果。这一信息确认系统主要包括三方面的因素：档案信息确认、身份确认和数字签名。三是档案信息网络控制技术。这一项技术主要包括四个方面，分别是防火墙技术、审计技术、访问控制技术以及安全协议。它允许用户对其常用的档案信息库进行适当的访问，但严格限制随意删除、修改或拷贝档案信息文件，并能及时发现并拒绝“黑客”的入侵。通过这些网络技术的应用，能够有效地保障档案信息的安全。

（2）美国是最早提出信息安全保障的国家。1996 年，美国国防部在国防部令 S-3600.1 就对信息安全保障作了如下定义:“保护和防御信息及信息系统，确保其可用性、完整性、保密性、可认证性、不可否认性等特性。包括在信息系统中融入保护、检测、反应功能，并提供信息系统的恢复功能。

美国在对档案信息的管理中，一方面十分重视档案信息安全，根据档案信息安全法律的规定来进行档案信息安全管理工作;另一方面，又十分重视档案信息的开放，主张档案信息应当为公众服务。

在档案信息安全的技术手段上,美国采用了两种方法:一是密钥芯片控制。首先，是对密钥芯片出口进行专项控制，通过对于对密钥芯片位数的控制来实现这一目的。例如，美国政府规定对中国的出口控制为 40 至 56 位，而商用芯片出口控制为 128 位。其次，美国政府对密钥芯片的算法采取了保密措施,明确规定对于商用的算法可以予以公开，但是在军用的算法方面则绝对不允许公开。第三，美国政府明确规定,美国所出产的产品必须在密钥芯片方面为美国政府留下一个接口，这个接口可以由美国政府来随时启动，这与就意味着凡从美国进口的计算机、交换机、路由器，均被美国政府控制着。二是采取了出口等级限制。1985 年，美国国防部发表了桔皮书—《可信计算机系统评测标准》，在这一套标准中，把计算机系统分为四个等级，八个级别，即 D(最低保护等级),C(自主保护等级)，B(强制保护等级),A(验证保护等级)四等，细分为 D，C1，C2，B1， B2，B3，A1，超 A1 8 级。并根据不同国家的情况出口不同安全等级的产品。通过这

些限制，美国政府的计算机机构及黑客进入其他国家网络可说是如履平地。通过这两种方法，有效地保护了美国档案信息的安全。

综上，加拿大和美国两国在保障档案信息安全方面都采取了通信安全技术和计算机安全技术。通信安全技术主要包括三种技术:信息加密技术——保障档案信息安全的最核心的技术措施;信息确认技术——通过严格限定档案信息的共享范围来达到防止档案信息被非法伪造、篡改和假冒的技术措施;信息网络控制技术——主要包括防火墙技术、审计技术、访问控制技术等。同时，在档案信息安全的系统保障方面，美国和加拿大都建立了较为完善的系统保障体系，有效地保护了档案信息的安全。

2.2 国家对档案信息安全工作的重视

近年来，全国上下高度重视档案信息系统的建设、档案数字化和档案开发利用工作。从档案信息化建设一开始，就离不开对档案信息安全的保护工作。

档案安全事关党和国家根本利益，没有安全保障就无法开展档案利用，因此，国家档案局在提出建立覆盖人民群众的档案资源体系、方便人民群众的档案利用体系两大体系之后又提出了建立确保档案安全保密的档案安全体系。2010 年 5 月，全国档案安全体系建设工作会议在四川召开，部署“建立确保档案安全保密的档案安全体系”，之后，国家档案局把“三个体系”建设作为当前和今后档案工作的主要内容和努力方向。2010 年 6 月国家档案局发布《数字档案馆建设

指南》，提出建设数字档案馆保障体系，确保数字档案馆系统安全和数字档案信息安全，指出要按照信息安全等级保护的要求，采用相应安全保障技术方法，配备必要的软硬件设施，达到二级(系统审计保护级)以上安全保护标准;2011 年 1 月印发的《全国档案事业发展“十二五”规划》，强调要加强档案安全体系建设，提高档案的容灾及灾备能力，确保档案安全。

2013 年 7 月，为贯彻确保档案信息的安全，国家档案局结合档案行业实际，根据《信息系统安全等级保护定级指南》（GBT22240-2008）等国家标准，组织制定了《档案信息系统安全等级保护定级工作指南》。这是档案行业较为系统性地对信息安全工作的一次梳理。根据档案行业特点，《指南》分析档案信息系统受到破坏时所侵害的客体，侵害的事项主要包括以下三个方面：

（1）国家安全方面。档案信息系统受到破坏后影响到有关国家政治、经济、文化、外交、科技、民族、宗教、安全等档案信息保管、利用、发布、展示的正常进行，进而损害国家政权稳固、国防建设、国家统一、民族团结和社会安定。

（2）社会秩序、公共利益方面。档案信息系统受到破坏后影响数字档案资源的真实性、完整性和可用性，致使国家机关政务信息发布、档案业务开展、办公等工作无法正常进行，进而侵害社会正常生产、生活秩序和公众获取公开信息资源、使用公共设施、接受公共服务等方面的合法权益。

（3）公民、法人和其他组织的合法权益方面。档案信息系统受

到破坏后影响到档案的移交、接收、管理、保存、查阅、利用、获取、公布、展示、捐赠等工作的正常进行，进而侵害公民、法人和其他组织的隐私、知识产权、物权、信息获取等方面的合法权益。

这三个方面都提到了利用或者服务，可见在利用过程中发生的信息系统被侵害、信息泄露或影响信息真实性、完整性和可用性现象，已经成为档案信息安全保护要重点关注的问题。

2014 年 5 月，中共中央办公厅、国务院办公厅印发了《关于加强和改进新形势下档案工作的意见》，再次强调要建立健全确保档案安全保密的档案安全体系。2016 年 1 月，为指导和规范档案部门进一步加强档案信息系统建设和管理，国家档案局印发了《档案信息系统安全保护基本要求》，从管理和技术两方面，详细地描述了在档案行业实施信息系统安全等级保护的要求。2016 年 4 月，为深入推进档案安全体系建设，国家档案局印发了《关于进一步加强档案安全工作的意见》，就进一步加强档案安全工作提出要求。特别是在档案信息管理风险治理方面，强调各部门各单位要在环境及设备安全、网络安全、系统安全、数据安全和数据载体安全等方面制定完善信息安全策略并贯彻执行。由此可见，从顶层设计层面，国家对档案信息安全越来越重视。

2.3 档案管理系统信息安全保护的基本情况

在档案信息化建设过程中，各级国家综合档案馆对档案信息安全的风险和隐患有了更为深刻的认识，信息安全保护意识不断加强，信

息安全保护方面的投入不断加大，积极应用各种信息安全技术措施和手段来保护档案数据安全。但由于地区差异和其他各类因素，各级国家综合档案馆信息安全保护工作发展不平衡且面临不少问题。一般来说，省级和部分市级档案馆因区域经济优势，人才资源丰富，容易获得新技术的支持，档案信息安全保护工作做得较好。而受各种客观条件的限制，部分市级和县级档案馆的档案信息安全保护工作还较为薄弱，存在较大的安全风险和问题。

关于各级国家综合档案馆档案管理系统的档案信息安全保护现状，可以从专用安全软件和档案管理系统本身安全性两方面来阐述。

就专用安全软件而言，由于各地档案馆的规模和经费条件不同，也导致档案馆安全软件配备情况参差不齐。部分经费较少的档案馆只安装部署了防病毒软件，而对于档案业务网络中桌面的管理、进程的监控、流量的管理、数据的安全保护等缺少相应的、专用的安全软件系统，难以应对现在日益复杂的各类安全风险。特别在县级档案馆，以上的问题更加突出，大部分县级档案馆安全投入不容乐观，档案信息网络规模通常都比较小、复杂度低，采用的信息安全软硬件产品较为单一。

目前，各级国家综合档案馆档案管理系统建设多数还是侧重软件的应用功能，对于安全方面考虑相对较少。档案管理系统由于大部分采用开放式的协议，因此存在着先天性的安全隐患，如：来自黑客、蠕虫、病毒、间谍软件的电子威胁，来自系统漏洞及“后门”、系统故障、人为失误、拒绝服务攻击、自然灾害的物理威胁，来自网络攻

击和网页篡改、失密和被窃的内容威胁等等。同时，对软件安全漏洞的查找比较依赖于第三方的测试。部分档案管理系统的日志审计方面功能较少，有些系统甚至没有对数据的增、删、改等操作配有完整的操作日志，并且许多日志不能起到追踪问题和审计的作用。系统的用户权限划分往往也不够规范、合理；用户认证方面，一般仅采取密码口令的方式，对口令长度、复杂度和更新频率等都缺乏有效的管理，而像数字证书等更加安全的用户认证方式采用的较少。同时，系统本身对于档案数据的安全保护不够，比如：数据权限的划分不够细致，所有用户都可以访问到档案数据，业务软件客户端比较容易将档案数据下载、捕获到本地计算机，在防下载、防复制、防拷屏等方面做得不够等。这些都带来了相应的风险隐患。

具体来说，各级国家综合档案馆在档案管理系统中，一般采用了以下的防控手段：

（1）权限控制

在档案管理系统中，一般通过设计合理的权限分配控制，使档案馆工作者和利用人员具备不同的访问权限，确保档案信息的安全。但是，目前不少档案管理系统的权限控制功能设计存在不够完善，权限的控制一般只针对系统的功能模块，往往不能针对档案数据进行访问权限控制。同时，访问权限的分配也没有时效性限制，对一些权限比较大的用户缺乏互相牵制和监督机制，使得有些用户比如超级管理员权限过大，不利于档案信息的安全管控。

（2）终端控制

对于计算机终端进行控制主要针对的是档案信息的传输通道和介质，采用的措施主要包括禁用U口、光驱或者只允许内部移动介质接入等等，防止从终端计算机将档案数据拷贝到移动硬盘、U盘带走。但对于拷出终端的文件一般没有进行安全保护控制，而且大部分允许用户终端通过刻录光盘拷走数据，这样就难以保障脱离内网终端后的档案数据的安全。

（3）电子文件封装

电子文件与电子档案管理系统一般通过对电子文件与电子档案进行打包封装等处理，使电子档案与其元数据之间建立可靠联系，一旦对电子文件发生了改动，系统能够自动识别。但目前在电子文件封装中存在封装包功能有限，而且存在封装包占用空间大等不足，特别是对多媒体文件封装效果不佳。

2.4 档案信息利用过程安全现状

随着档案信息化的飞速发展和各级国家综合档案馆数字档案馆的建设，社会公众对档案查阅和利用的需求也日益增长，各级国家综合档案馆也通过各种手段，使档案的借阅和利用愈加便捷，档案利用工作发展迅速。

档案信息利用是档案价值的呈现，信息安全保障工作是其生命基石。在档案信息安全中，尤为重要的是档案信息利用过程当中的安全。在档案信息利用安全方面，由于档案利用安全涉及到档案信息系统调阅过程、离线利用过程、对外发布过程等，目前各省档案信息系统在

档案信息利用过程中尽管已采取部分安全措施，但基本还是侧重于对外部的安全防护方面，如：在档案数字化加工和档案网站系统建设中采取了一些安全措施，而对于档案信息利用过程整体安全防护的理解、认知和投入上都远远不够，现状如下：

（1）档案信息传输过程安全现状

档案馆借助政务网接收电子文件和电子档案时，多数只通过政务网网络安全设备对传输行为进行简单的访问控制、病毒监测和入侵防御等，有部分省份做到了 CA 认证。而对电子档案传输过程中的防窃听、防篡改等未采取有效的安全措施，对电子档案的完整性也缺少验证机制。

（2）档案信息馆内查询利用过程安全现状

档案信息的馆内查询利用流程一般包括档案检索、调阅等步骤。目前，大部分档案馆都提供了查阅大厅供查档者使用，在档案信息调阅过程中，有些档案馆采用的是直接下载到本地终端计算机的方式。档案信息在编研过程中编研人员可对内容进行拷贝、截屏、截图等并编辑成新的文档，脱离档案管理系统的控制。对借阅终端的安全管理方面各个档案馆目前一般缺少有效的安全管控措施。

（3）离线利用安全现状

档案信息在某些情况下通过审批以后，可以以离线方式下载到调阅者主机或移动存储介质上。目前，只有极少数的综合档案馆对档案信息离线利用采取措施进行安全防护，这样脱离系统的档案信息就会失去档案管理系统和档案管理者的控制，是否被多次复制、是否被非

授权人查看、是否被扩散泄密等都无从追踪和审计，因此存在着风险。

（4）档案信息对外发布安全现状

各级国家综合档案馆一般通过自建网站、内容托管等方式，向社会公众提供开放档案信息查询，或依据某个特定的业务系统向有权限查阅的用户进行主动的分发。目前，档案网站和档案业务系统基本都能按照信息系统等级保护的要求进行安全防护，问题主要存在访问权限及内容防扩散上，特别是需要授权访问时，如何确保访问者身份和合法性，以及在档案信息主动分发时缺少考虑传输过程的防窃听、防扩散等问题。

目前，为保障档案信息的安全，各级国家综合档案馆都在积极实施档案信息系统安全等级保护工作。尽管安全等级保护为信息系统的安全提供了有力的保障和分析工具，但是由于其着重于解决网络和基础层级的安全问题，没有充分结合应用的场景，因此对档案信息安全来说，还存在着安全短板。具体来说，在档案利用环节的安全短板主要体现在：

(1) 无法有效防止档案的泄密。传统的安全防护无法识别档案数据本身的敏感程度，无法从应用和业务层面来判断数据的类别和使用权限等信息。

(2) 无法控制用户对脱离系统的档案文件的操作。用户对档案文件的操作依赖于系统权限，需要从业务层面赋予策略，结合安全技术实现细粒度的控制。

(3) 无法监控和审计档案文件的行为。所有的安全风险均通过行

为产生，现有的安全措施无法监控、跟踪和审计对某一档案文件的具体操作行为，从而形成风险。当档案数据出现失泄密现象时，难以追查是哪个环节出现了问题。

(4) 安全状态不可视。档案馆虽然部署了很多的安全设备，采取了很多的安全措施，但是对档案利用环节的档案信息的安全状态还是无法直观感知，档案信息遭到破坏或窃取无法第一时间知晓。

综上，从总体上来说，档案信息利用安全保护现状是不平衡的，存在区域性、环节性的不平衡，尤其是在对内部利用和离线利用等环节较少采取有效的安全防护措施，与国家安全战略及《网络安全法》的要求差距较大，缺少全过程风险评估，对档案利用全过程缺少统一和长远的安全规划，更缺乏相关的安全功能设计，这是各级国家综合档案馆普遍存在和急需解决的问题。

2.5 档案信息利用过程安全风险

风险是指损失的不确定性，对档案信息而言，风险指的是可能出现的影响档案信息安全的不确定因素。要从安全保护的角度去考察档案信息，不能停留在静态的一个点或者一个层面上。电子文件与电子档案是具有生命周期属性的，在利用过程中也是生命周期的一个缩影，也包含着许多环境，各个环节各个阶段都应该被考虑到，安全保护应该兼顾在利用过程中档案信息可能存在的各种状态，不能够有所遗漏。因此，有必要结合文件生命周期去进行分析。具体地，我们根据电子文件与电子档案生命周期的各流程，结合档案信息应用场景，

大致将利用过程分为：系统调阅、对外发布和离线利用等。每个过程的风险点大致分析如下：

2.5.1 档案信息系统调阅安全保护风险分析

系统调阅指的是在档案信息管理系统内对电子档案信息的调阅（不包括政务网和互联网站上的应用）。一般可以根据档案利用者的不同划分为档案馆内用户的利用和档案馆外用户的利用。

档案馆内用户的利用过程一般包括档案信息的检索、调阅等步骤。

（1）检索方面，一般通过档案信息管理系统可以对档案信息进行分类检索、跨类检索、全文检索等，这其中涉及到授权查看数据的问题。如果权限划分不清或者划分不细，可能产生档案数据被非法查看的问题。如有些档案馆对档案数据没有进行准确分级，对馆内用户实行系统中所有档案数据一律可查，就存在着保密数据被非涉密工作人员查看等风险隐患。

（2）调阅过程涉及两个步骤，一是数据传输，二是数据浏览。

由于目前档案管理系统主流采用 B/S 架构，因此数据传输基本上是以网络传输的方式进行的。通过网络进行档案数据的传输，具有以下的风险点：

a.数据传输途中数据可能被窃取、修改、破坏等。不少地方档案信息的流转还采用明文方式传输，增加了网络传输过程中数据被监听窃取的风险。

b.数据传输端、接收端的用户仿冒问题。尤其是档案数据传输的身份认证多数还依赖口令这种传统方式，数据的传输通道较少使用加密技术，这种情况下用户身份更容易被冒用。

c.有些档案管理系统采用的是将档案信息直接下载到本地终端的方式，这种方式有很大的风险性。而且，档案管理系统中的档案信息在点击下载到终端上查看和操作时，档案信息处于明文状态，由于用户终端或信息网络存在安全和管理的脆弱点，容易造成档案信息外传导致信息泄密。而且，一旦档案信息被下载后可以随时传播，在缺乏终端防护的情况下，无法跟踪文档的使用和去向，特别是第三方系统对电子文档的利用。终端电脑对档案信息的使用期限、次数、拷贝等行为无法被控制和跟踪审计，造成很大的安全隐患。同时，一些档案安全意识不足的工作人员，档案信息下载后与个人文件数据混杂在工作电脑和移动介质中，甚至放到连接互联网的电脑上，很容易被病毒、木马程序窃取或通过邮件等方式流传到公众网络中，导致档案信息信息被外泄。

数据浏览过程中档案信息容易被拷屏、拍照、打印等造成泄密，有些档案管理系统架构过于简单，采用一般网页浏览的方式，很容易被用户以“图片另存为”等方式拷走档案信息，而且不会留下记录。这样导致事中无法进行审计和警告，事后无法追踪泄密的源头，带来很大的风险隐患。

（3）档案信息的编辑可以分为鉴定整理部门对档案目录信息的编辑和编研部门对档案信息内容进行加工的过程。编辑过程中除了有

一般检索、调阅的风险外，还有以下风险点：

在鉴定整理部门的编辑过程中，由于缺乏对档案数据权限的管控，可能存在超越权限的操作，或者误操作导致的风险，甚至导致电子档案信息被篡改；某些档案信息没有加密，可能很容易被查看，目录信息更容易被复制到本地终端计算机上。

在档案编研过程中，除了以上问题外，还由于可以对电子档案内容进行拷贝、截屏、截图等并编辑成新的文档，脱离档案管理系统的控制，从而导致从系统中获取没有下载权限的重要档案信息。因此，防止通过编辑生成的新文件中的重要信息外泄是编研过程中必须考虑的问题。

档案馆外用户利用的需求类似于档案馆内用户的利用，也存在着档案检索、调阅等利用风险。由于面向外来利用人员，情况会更加复杂，外来利用人员可能会携带各种设备进来，而且人员的身份可能不明确，这一切都会给档案利用工作带来相应的风险。

2.5.2 档案信息对外发布安全保护风险分析

档案信息对外发布一般可以分为两种，一种是在政务网或互联网站上发布公开的档案信息；另一种是依据某个特定的档案管理系统，向有权限查阅的用户进行主动的分发共享。

首先，目前在政务网或互联网站上公开发布的档案信息，有可能出现由于审批不严、误操作等发布了不该发布的档案信息的风险，同时，由于网络具有联结形式的多样性、开放性、互连性等特征以及档

案信息本身所具有的敏感性、价值高等特点，致使其易受黑客的攻击和病毒的入侵，造成档案信息的泄密、假冒、篡改等诸多问题。

其次，依据档案管理系统的分发共享同样存在系统检索、调阅等可能存在的问题。主动的分发共享，还存在着信息分类不当，或者没有按照相应权限分发档案信息的共享，而且在分发过程中，也涉及档案信息的传输风险。同时，档案信息传输到相应用户后，在用户的终端或者平台上，能否确保不泄密、不外传，也是存在一定的风险性。往往分发给用户之后，无法控制用户的二次传播，容易被复制甚至篡改，或者被黑客、木马等窃取。

2.5.3 档案信息离线利用安全保护风险分析

档案信息离线利用，特指档案信息脱离档案管理系统后的各种利用。现实情况下，档案信息经常存在着导出系统提供利用的可能，脱离系统后的档案信息更存在被非法复制、篡改和传播的风险。而且，由于信息已经离线，缺乏对工作计算机和移动介质的控制管理，可能导致档案信息未经批准被带离档案馆，造成被病毒、木马程序窃取或通过邮件等方式流传到公众网络中，导致档案信息外泄。

同时，离线调阅一般通过存储介质进行，存储介质在携带、使用时，往往缺乏标识认证和访问控制，导致移动介质无法安全管控。而且，这些存储介质若损坏或丢失，都将带来巨大的损失和外泄事件的发生。

对档案信息在利用过程中的安全防护是一项整体的工作，由于安

全风险点普遍存在于档案信息利用过程的各个环节，因此要对以上的这些档案信息利用过程中的需求进行统一考虑和规划，使之在同一的安全管控之下实施，又能根据各个过程的特点有所侧重，使得安全防护工作成为一个有机的整体。这些都是功能需求方案中必须要考虑的问题，我们将在下一章进行阐述。

第三章　各级国家综合档案馆电子文件与电子档案管理系统在档案信息利用过程中安全保护功能需求方案

3.1 档案信息安全保护相关理论

本章讨论各级国家综合档案馆电子文件与电子档案管理系统在档案信息利用过程中安全保护功能需求方案。由于利用过程中的档案信息安全具有动态性、复杂性、相对性的特征，因此要对利用过程中的风险进行充分有效的分析评估，在了解风险点的基础上，评估这些风险可能带来的安全威胁与影响程度，从而提出相应的功能需求方案。因此，档案信息利用过程中的安全保护可以基于风险管理理论，并根据档案的特性，结合文档生命周期理论，从动态的生命过程中进行技术实现方式的构建，以达到档案信息利用过程中主动性、动态性、全过程安全管控的目的。

3.1.1 风险管理理论

上一章提到了档案信息利用过程的安全风险，因此需要进行风险管理。风险管理是为了达到一个既定的目标，而对所承担的各种风险进行管理的系统过程。它是由风险评估、风险处理以及基于风险的决策所组成的完整过程。风险管理的基本要素包括：使命、资产、资产价值、威胁、脆弱性、事件、风险、残余风险、安全要求、安全措施等。各要素之间的关系如下图所示：

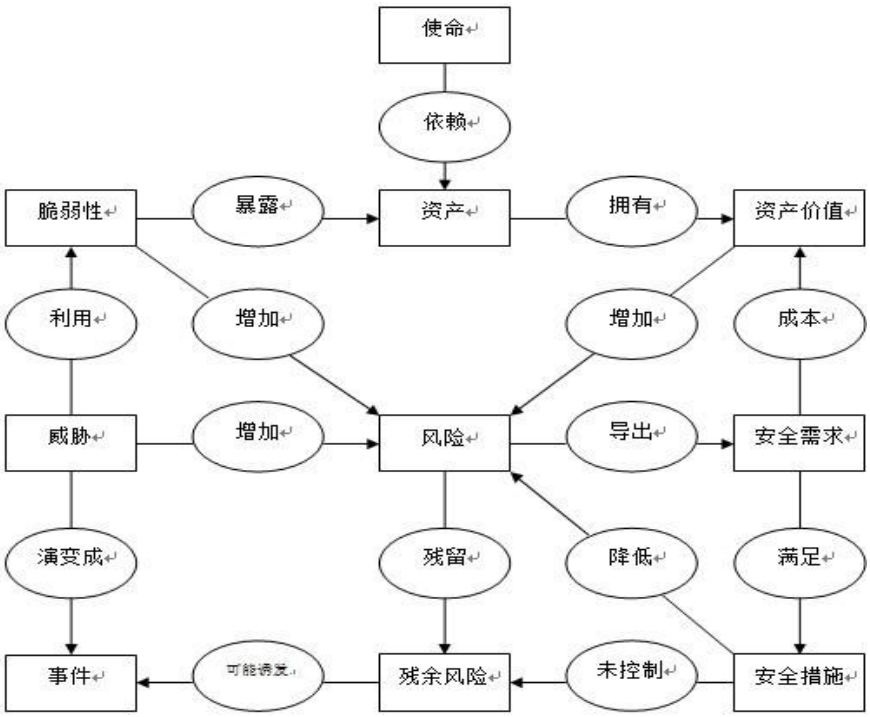

图 3-1 风险管理各要素之间的关系

风险的实际水平可以由威胁的可能性乘以其影响得到，如将威胁可能性分别设为高（1.0）、中（0.5）、低（0.1）三级，将威胁的影响分为高（100）、中（50）、低（10）三级，可得到如下风险矩阵：

威 胁 可能性	威胁影响		
	低（10）	中（50）	高（100）
高 （1.0）	低 (10x1.0=10)	中 (50x1.0=50)	高 (100x1.0=100)
中 （0.5）	低 (10x0.5=5)	中 (50x0.5=25)	中 (100x0.5=50)
低 （0.1）	低 (10x0.1=1)	低 (50x0.1=5)	低 (100x0.1=10)

风险等级：高(50-100)、中(10-50)、低(1-10)。

因此，对档案信息利用过程中的风险进行分析时，不仅要针对危险的威胁性、产生的后果进行分析，还要对风险发生的可能性进行预测，从而达到动态、准确的安全防护。

风险管理的流程如下：

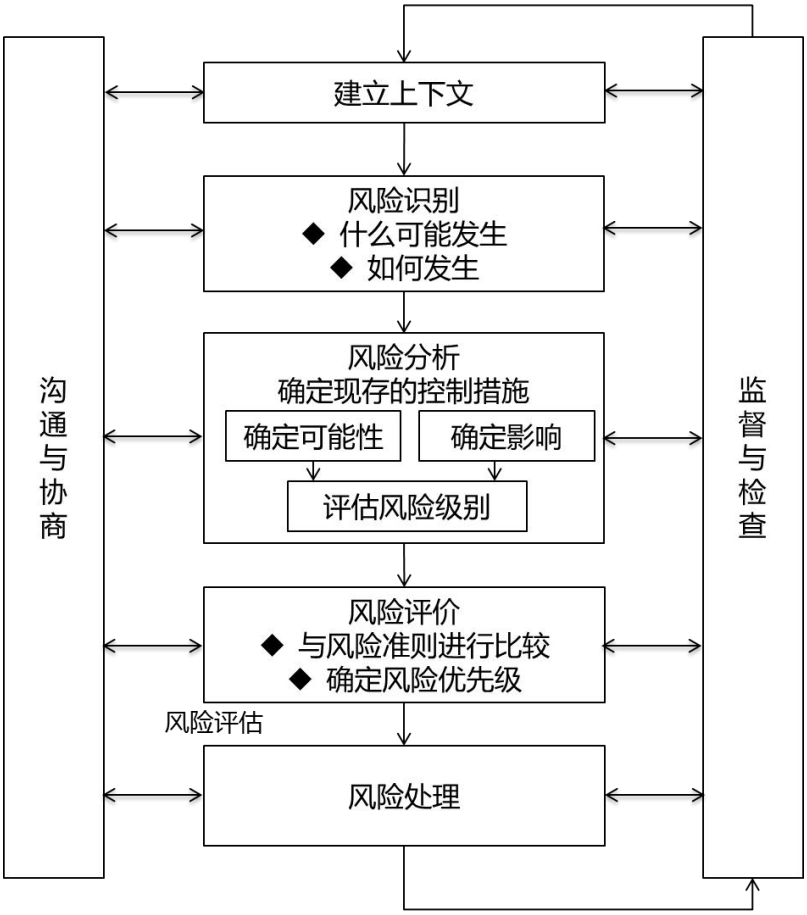

图 3-2　风险管理流程

结合风险管理的理论，可以对档案信息在利用环节的安全风险进行识别和定义，使用监控、阻断、告警等处理措施，对高风险、非法的操作行为进行响应。其安全管控流程如下：

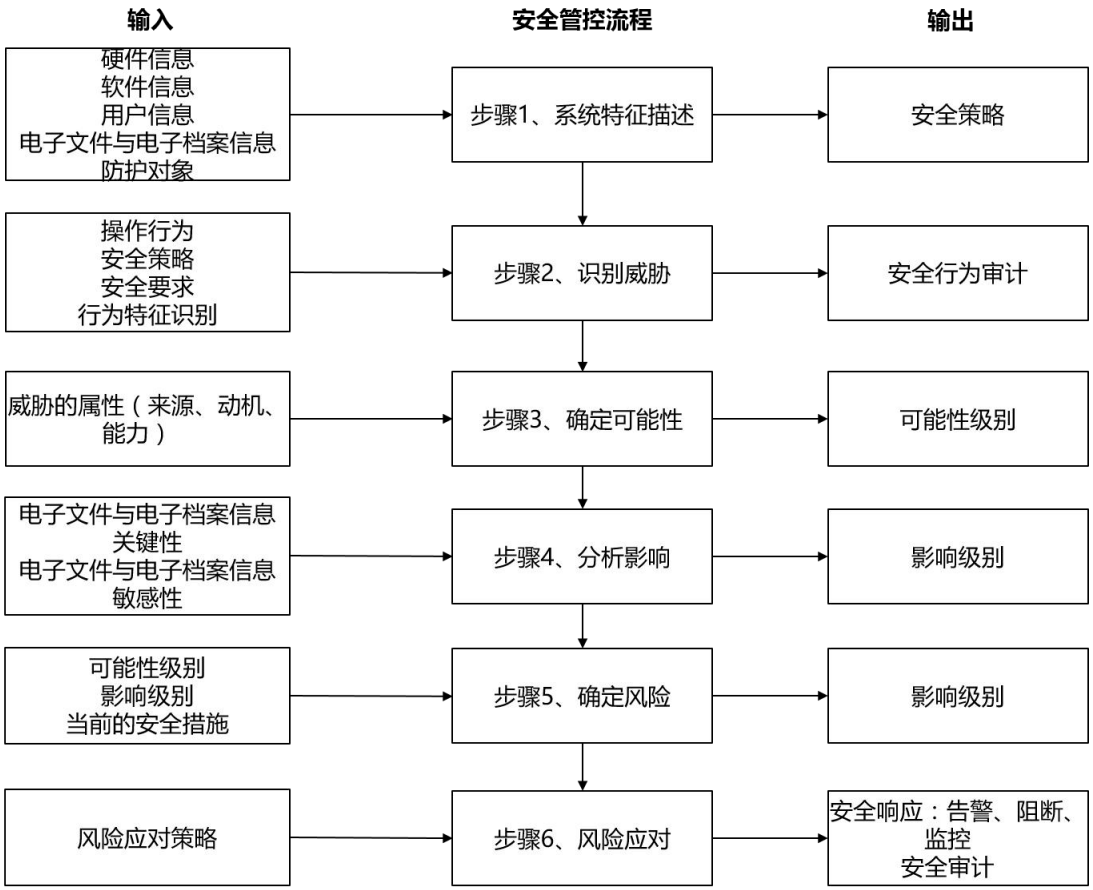

图 3-3 档案信息利用安全管控流程

3.1.2 文档生命周期理论

档案学者菲利普.布鲁克斯提出的“文档生命周期”概念，是指“文档从生成直至因丧失作用而被销毁或者因具有长远历史价值而被永久归档的整体运动过程”。文档从产生的那一刻起就自然赋予其生命，经过生成、使用、存储、销毁过程。电子文件及电子档案符合文档生命周期理论，因此可以提出电子文件全生命周期的逻辑安全域。

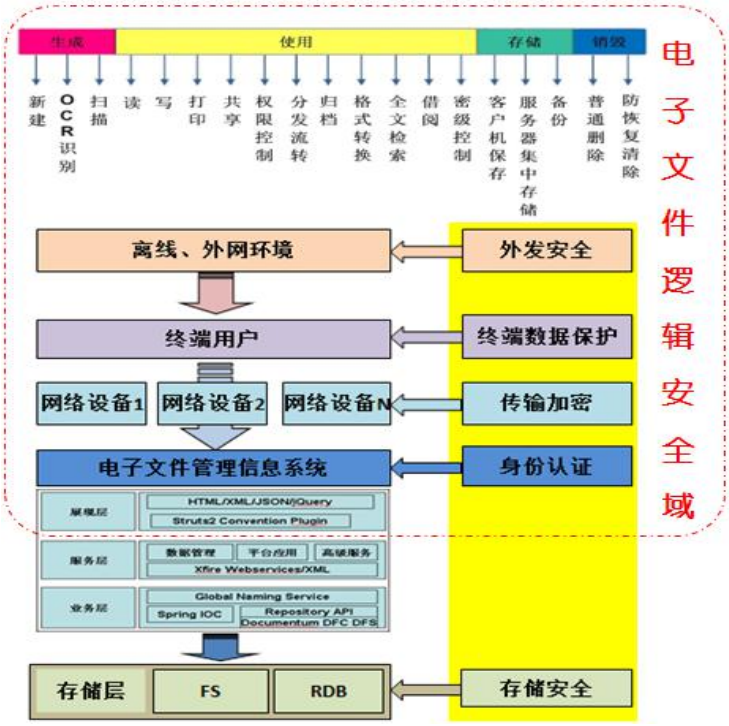

图 3-4 电子文件逻辑安全域示意图

在电子文件全生命周期中，档案信息的利用位于与用户交互的层面，是整个生命周期的核心环节。可以看出，电子文件一经生成，其相应的档案信息随后就存在着被利用的可能。前面指出档案信息利用的具体场景，可以大致分为系统调阅、对外发布、离线利用等；同时，按数据流转方式可分为后台存储、系统调用、网络转输、终端使用和外发控制五个阶段；因此，它的安全域框架就是以档案信息为基本单位，生命周期相应的系统内所划定的与其权限和使用范围相一致的逻辑区域，也就是档案信息被授权使用的边界或对象。电子文件与电子档案管理系统中的档案信息安全可以遵循此安全域设计框架对档案信息安全进行全方位的保护。

从生命周期理论考虑利用过程中的安全保护，还有一个启发，就

是要尽早地考虑到档案信息的分类和统一的安全策略，甚至在档案信息收集时就应当考虑，因为作为一个生命周期的延续体，前期的分类和安全策略如果设置不当，后期也就无法进行有效地管控。而分类也涉及相应元数据的收集，这些工作也需要尽可能在前端完成。

3.2 安全保护原则

各级国家综合档案馆在实施档案信息利用过程的安全保护中，应当遵循以下原则：

（1）整体性原则：在档案信息利用过程中，应当注重系统的、整体地对信息安全进行防护。由于档案信息安全涉及面广，每个过程的风险都会影响整体的安全性。信息系统是一个复杂的系统，物理上、操作上和管理上的种种漏洞构成了系统的安全脆弱性，同时，档案信息自身的复杂性、资源共享性使单纯的技术保护防不胜防。因此，要尽量通过多种手段的配合消除各自的不足，从整体上设计功能需求方案，对信息系统进行全面均衡的保护，提高整个信息系统的安全性能，保证各个层面防护上的均衡。

（2）规范性原则：在档案信息利用过程中，要制定相应的标准和规范，遵循国家关于信息系统安全的相关标准和规范，同时符合档案行业安全保护的相关要求。在档案信息系统功能设计时应遵循统一的规范要求，实现档案信息管理和利用工作的有序化、标准化和规范化。

（3）主动性原则：与一般被动的静态安全保护不同，档案信息

利用过程中的安全保护要求应能够对在利用中可能产生的操作以及带来的风险尽可能进行预判，从而进行积极主动的防御。如事先考虑到档案用户复制电子档案操作的可能性，从而可以在技术上直接根据用户的权限和文件的属性进行相应的安全保护。

（4）动态性原则：档案信息利用过程是一个动态的过程，各种应用需求和条件可能在不断发生变化，如对不同种类和年限的档案信息及其载体，安全保护的要求是不一样的，此时安全不代表以后安全。安全保护系统要考虑到这些因素变化的差异性，从而有针对性的进行安全保护。

（5）扩展性原则：档案信息安全保护实现应具有高可扩展性，能够与档案馆现有的信息安全设施设备进行无缝集成，能够与第三方安全设施和技术兼容。在档案信息系统建设时，要充分考虑未来档案信息管理和利用中不断增长的业务需求，并具有向未来技术平滑过渡的能力。

（6）安全性原则：安全保护的核心目标是保障档案数据的安全，因而安全保护系统本身的设计也要注意安全性，要把所有安全因素考虑在内，尽量选用经过大量运用、成熟的经过实践检验的技术和产品，避免对档案信息系统和档案数据造成任何影响，以保证档案信息的绝对安全和档案信息系统运行的连续性。

3.3 安全保护目标

档案信息利用过程中安全保护的目标，就是要采取措施（技术手

段及有效管理等）让档案信息资产免遭威胁，或者将威胁带来的不良后果降到最低程度，同时维护档案信息的正常利用。要从根本上解决档案信息在利用过程中的安全问题，确保档案信息的安全可靠，重点应从以下几个方面来考虑：

（1）保密性（Confidentiality）：通过安全技术措施和安全管理制度的建设等保护档案信息，授权给合法用户使用，控制对档案信息进行的不同操作，如控制有浏览权限的人是否能复制、打印、摘录、传播等，从而保证敏感信息不被泄漏，确保档案信息在存储、使用、传输过程中不会泄漏给非授权用户。

（2）完整性（Integrity ）：确保档案信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，确保档案信息不会由于时间的消逝和恶意的损害而导致丢失、损坏等，保持信息内、外部表示的一致性。本属性可进一步衍生可追溯性（Accountability ）、抗抵赖性（Non-repudiation）和真实性（Authenticity）。

（3）可用性（Availability ）：确保授权用户对档案信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问档案信息及资源。因为利用过程中的安全保护最终的目标还是要落脚在利用上，因此，对于正常的利用必须予以保障。可用性也表示档案信息的内容是来源可靠的，不是被伪造的。