3.4 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

前面提到，安全防护工作应成为一个有机的整体。依据风险管理和文档生命周期理论，根据档案信息利用过程中的安全保护原则，我们认为，应当将档案信息利用安全的功能扩展到收集整理、存储传输等领域，从前端把控好权限和数据的分类，从而整体上推动档案信息利用的安全。另外，由于系统调阅过程涉及到的功能点较多，我们将一部分功能与离线利用合并，归于信息公布功能，因此，最终将档案信息利用安全的功能大致分为收集整理、存储传输、查询利用、信息公布、对外发布等方面。同时，在每个具体的过程中，通过事前、事中、事后的功能需求分析，围绕安全保护目标，从整体上系统设计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的功能需求方案。其中：事前防范主要是指通过安全策略的设定，事先防范安全风险。事中控制主要是指通过对操作过程的控制以及对其中档案信息的控制来实现过程中风险的规避、发现和告警。事后审计主要是指在档案信息利用过程中发生的所有行为，包括用户行为、设备行为以及网络行为等，进行审计跟踪，做到事后可以追溯。具体的事前、事中、事后在档案信息利用的每个环节中侧重点有所不同，我们将结合具体的环节进行详细阐述。

3.4.1 收集整理

我们把档案信息收集整理纳入研究的范畴，一则是由于在收集整

理中也涉及到档案信息的利用，如在数字化加工中对原有档案目录数据的使用；二则是从全生命周期来看，如果在收集整理时没有做好相应的分类，捕获必要的元数据等，就会对后面的档案信息利用过程中的安全带来风险隐患，因此我们在这里简要地论述下收集整理方面的功能需求。

收集，一般包括电子档案接收和传统载体档案数字化转换这两个方面，其他的收集渠道虽然五花八门，但最终也要通过这两个步骤才能进入系统。整理，这里我们特指与收集相关的对档案数据的整理。因此我们分别概述需求如下：

3.4.1.1 电子档案接收

在电子档案接收流程中，各级国家综合档案馆要对电子档案进行解密、解压缩、验证签名等，经检验合格的电子档案才能入库。这个检验的过程非常关键，目前一般强调电子档案数据的准确性、完整性、可用性、安全性四性检验。通过四性检验，既避免了有病毒或木马的档案数据进入系统，同时保证了档案数据的准确、完整和规范，便于下一步进行数据权限的管控。四性检验不合格的电子档案数据要及时退回到形成单位，并附上相应表单，标记所缺要件或不符合接收规范的原因等。

除了四性检验外，为保证电子档案的安全，从需求上来说，在电子档案接收中还应当做到以下几点：

（1）事前，应启用访问控制功能，依据安全策略控制档案用户

对资源的访问，仅授予用户所需的最小权限；应当采用有效的身份认证技术，防抵赖、可追踪；减少档案用户在接收过程中的不必要操作，避免因误操作带来的风险。

（2）事中，应建立安全的传输通道，对传输内容进行加密。当电子档案迁移时需要保证在传输中安全，避免被非法窃取或信息完整性被破坏。传输通道要采用加密协议，最好能指定点对点传输，在传输之前，先确定对方的身份，同时保证传输的过程不被窃取、篡改，或者被窃取后的文件是不可解密的；应实现对档案信息存储空间的安全防护，避免非法入侵和篡改数据，或者数据由于硬件问题而损毁、丢失。

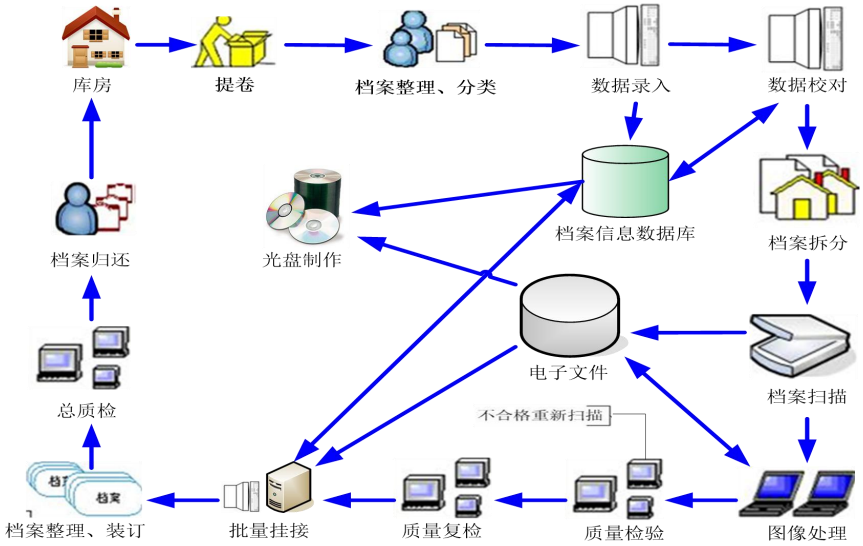
（3）事后，要加强对电子档案操作的审计，尤其要注意对电子档案的四性检测结果进行审计，以保障档案数据的安全和规范性。根据审计结果，各级国家综合档案馆可以对各立档单位和相关人员提出相应的整改要求。

3.4.1.2 数字化转换

目前，很多国家综合档案馆在档案数字化转换时选择服务外包的方式，在档案数字化加工过程中可能涉及到较多的外部人员，在档案扫描、图像处理、数据质检、数据挂接、数据迁移、光盘备份等环节中都可能存在数据被拷走或被拍照的风险。如果缺乏对数字化过程中敏感和危险操作的记录和审计，数据被盗或泄密后也难以追查。

其次，档案数字化过程并不是一个瞬时工作，而是需要一个较长

时间的转换过程，扫描后的数据文件会保存在扫描仪、图像处理软件等应用软件及设备中，同时加工后的档案信息一般直接保存到文件服务器或以光盘、移动存储介质形式进行备份存储。这些存储介质如果缺乏应有的管控，可能会档案信息的损坏或丢失，并存在被非法拷贝的风险，都将带来巨大的损失和外泄事件的发生。



数字化加工流程图

因此，在档案数字化加工过程中，各级国家综合档案馆应加强对档案信息的安全保护：

（1）事前，应建立完整、严格的数字化安全管理制度，并设计一整套统一的针对数字化加工的认证体系，任何人未经认证无法登陆和访问档案信息。

（2）事中，对数字化加工的各个环节分配不同的权限，每个账号只能由本人使用，严禁串用。同时，加强对数字化人员、场地和设

备的管控，不允许任何人员带入手机、计算机、U 盘和数码相机等。只允许人员采用专用的、已标识过的设备，并对存储输入和输出口 r（USB、串口、红外、Wifi 等）进行管控。建立数字化加工设备台账，严格落实登记制度，如设备损坏或报废，应由专门人员进行处理。数字化加工网络应单独建设，与档案馆的其他网络物理隔离。

（3）事后，对整个数字化过程中的敏感和危险操作记录进行审计，便于监控和追查。

（4）事中和事后，安排专人统一接收数字化加工完成的档案数据，并设置相应的数据备份措施，防止数字化加工成果丢失。

3.4.1.3 数据整理

档案数据整理功能主要涉及事先的规则定义、事中的操作管控和事后的行为审计。在档案数据整理环节，需要按照预先设定好的权限进行，并且要经过相应的审批流程。同时，对档案数据的整理，应当按照相应的标准来进行（如《档案著录规则》等），这点可以通过将标准内嵌入档案信息系统来实现，当人工作出不符合系统设定标准的整理时，系统应予以警告或禁止，这些是为了保障档案信息的规范性，从而在其他阶段可以根据档案数据整理的结果进行相应的权限管控。数据整理后，要保存完整的档案数据整理记录，同时要由专人或专业的系统对记录进行审计分析。

3.4.2 存储传输

由于在档案信息利用过程中多多少少都涉及到数据存储和传输

的问题，因此，我们在这里集中探讨数据存储和传输的安全保护需求。

3.4.2.1 数据传输

档案数据传输的安全功能需求包括以下几点：

（1）用户身份认证

档案信息系统对要求进行档案数据传输的用户应进行身份认证，结合系统的权限管理，避免非法的传输申请。

（2）文件分块、断点续传

档案信息系统应根据网络情况、文件大小等对需要传送的文件进行智能分块传送，并支持断点续传及自动重组。

（3）不改变文件属性

对传输中的文件保持其文件属性，包括创建时间、最后修改时间等信息，这样可以用于事后跟踪、备查，并且这些文件信息能被读取到系统数据库中，作为传输文件的文件属性保存。(如:电子档案创建时间等)

（4）网络带宽智能检测

针对网络情况，档案信息系统应设置网络带宽智能检测，传输带宽满足一定带宽的时候启动或中断传输，并且可以设置上传的速率或满负荷传送，支持在网络不通的状态下设置传输任务，一旦网络正常则启动传输或定时传输。这样可以减少传输过程中的堵塞问题并且防止恶意传输。

（5）传输过程加密

档案信息系统应建立安全的传输通道，传输通道要采用加密协议，最好能指定点对点传输，使用户在传输之前，先确定对方的身份，同时对传输内容进行加密，保证传输的过程不被窃取或信息完整性被破坏。

（6）监控日志审计管理

档案信息系统的监控日志要跟踪传输情况，可以根据传输内容、传输类别、传输单位或个人、传送数量、传送效果等信息进行有效的查询、汇总、统计、生成报表，并可以根据需要形成月度报表、季度报表、年度统计等报表。通过审计分析，及时发现传输过程中的问题，并在下一次传输前予以调整。

（7）实时状态管理

档案信息系统应对数据传输的实时状态进行管理，设置实时查询传输情况、传输状态，实时显示传输文件、传输流量等信息。对传输过程以及传输结果中遇到的各类情况实时告警，包括：连接速率、传输过程网络故障、传输端对服务器的网络攻击行为、传输文件不完整、传输文件破坏或感染病毒、传输端被篡改等信息，并根据严重程度做出不同等级的告警，不同的告警信息用不同的颜色予以区分。

3.4.2.2 数据存储

档案数据存储要保证数据层面的安全，一方面，通过采用现代密码算法对数据进行主动保护，如：数据保密、数据完整性、双向强身份认证等；另一方面，主要通过采用现代信息存储手段对数据进行主

动防护，如：通过磁盘阵列、数据备份、异地容灾等手段保证数据的安全。

1.存储策略

首先要建立规范合理的数据存储策略,明确档案数据的分库以及各自存储的位置、采用的存储方式和载体，建立并落实定期的数据监测、备份、迁移等内容的数据存储管理制度。

其次，存储空间的访问应设置权限，非数据库管理员无法访问存储空间，避免普通用户通过远程连接直接登录到后台的存储空间。

2.数据真实性

档案数据在存储时应为每份原文生成唯一摘要码或验证码,并存放在数据库中，可以实时对原文情况进行比对，确保原文内容与产生时一致，未被篡改，信息无丢失。

3.数据完整性

应能够检测到档案信息以及系统相关数据在存储过程中一致性、完整性受到破坏的情况,并在检测到完整性错误时采取必要的恢复措施，确保数据的完整性。

4.数据保密性

应采用加密或访问限制与监控等其他保护措施实现档案信息以及系统相关数据的存储保密性。

5.长期保存性

档案信息存储应采用符合相关标准的通用的格式,并存放在符合国家有关标准规范的环境中。

6.备份和恢复

应提供档案信息的数据备份与恢复功能，根据数据情况定期进行备份和迁移，备份介质场外存放；提供档案信息的异地数据备份功能，利用通信网络或人工方式将关键数据定时批量传送至备份场地；采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障等问题；提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

3.4.3 查询利用

档案信息查询利用是最主要的一种利用形式，它指的是用户通过档案信息管理系统对档案信息进行查询、浏览乃至一定的输出（如复制、打印等）等方面的利用。档案查询利用方面的功能需求主要包括以下几点：

3.4.3.1 利用登记注册

在档案信息查询利用前，利用者的信息要经过登记，新增用户要经过申请、审批、反馈的流程。同时，系统应具备身份认证、用户设置与权限分配等管理功能。

在档案信息利用时，应当按照实际情况设置相应的利用者角色和审批流程。审批应由档案利用的管理人员执行，并对审批过程进行记录。首先，要根据各种人员级别、层次进行使用权限的认定，并依此向利用系统注册登记。其次，在档案信息利用上，要根据档案信息的

密级和开放程度，来确定其使用控制程度，系统要能够控制到每个电子档案或每条档案信息的操作控制权限，操作控制权限可以定义在一定的期限内、或某个固定终端上，可以进行操作种类等等。尤其，对于外来人员，应当进行有效的身份确认，如用身份证、工作证、介绍信等进行确认。外来利用者用户的临时账号，应当具有授权有效时间、指定专用计算机的限制。

系统在设置相应的访问权限时，应遵循以下几点：

（1）最小特权原则。规定用户应当只被授权访问那些完成其指定工作任务所需的最小权限，也就是说，应当阻止档案馆用户访问那些与其工作任务无关的内容。按工作需要能够赋予最小权限的就赋予最小权限，不得赋予超出工作需要的权限。而当用户想要访问超出其权限访问内的档案信息时，系统应能直接禁止并进行告警，并同时通知系统管理员。这样做到用户只能访问修改其工作任务要求修改的那些数据文件时，就确保了系统中的文件保密性和完整性。

（2）“知其所需”访问。在特定的分类级别或安全域内，某些档案信息可能会被划分或间隔化，使得对这些档案信息的访问有所限制，只有当用户能够提出与工作任务相关的合理访问理由，或能够证明“知其所需”访问的正当性，才会被授予访问权限。“知其所需”访问由应档案馆主管部门依照审批手续决定，并且只授予有限时间的访问权限。

（3）分权制约原则。该原则是针对管理员的，一般来说，重要的档案信息管理系统，不允许超级管理员的出现，通过合理的划分管

理员权限，使系统管理员、数据库管理员、安全审计员等之间相互牵制，避免管理员的一些违规行为。

3.4.3.2 操作过程管控

在档案信息查询利用时，应结合权限分配，启用访问控制功能，依据安全策略控制用户对档案信息资源的访问。系统授权用户对受保护的档案信息进行操作时，操作权限受到统一安全策略和档案信息状态的控制，包括查看时间、查看次数、截屏等。对档案目录和全文的检索应该有所区分，对档案信息在不同网络的浏览应该分别予以管控。高级别操作权限应当通过审核、审批来实现授权，保证对档案信息进行不同的操作时，仅授予用户最小的权限，从而确保敏感信息不被泄漏。

在档案信息利用的动态过程中，由系统自动判定当前使用者身份的合法性及其所使用功能的范围，并由系统自动对其使用各种功能操作的路径进行跟踪与记录，对涉及使用未经授权的功能，应能拒绝响应并给予警告提示。如检索过程中，可根据检索者检索的档案类别权限设定控制，防止检索非授权的档案类别数据。

同时，应禁止非认证的应用程序对档案信息的操作，避免加密的档案信息被另保存为非加密信息。对不开放的档案信息，应当能严格控制利用，确保档案信息的安全。

3.4.3.3 文件内容保护

在档案信息查询利用前，应通过版权控制管理技术保护电子档案

信息，对系统中的档案信息绑定版权信息，防止其信息被拷贝，并使得对文件的保护不依赖于网络、系统或存储介质。同时，通过摄像监控、利用电子水印等技术防止档案信息内容被拍照。

同时，在档案信息浏览时，应能设置允许浏览时间，并能控制浏览原文的页码，如：一个原文共有 10 页，可以只提供其中的第 2 页和第 3 页给利用者浏览。还可以设置浏览密码等授权认证，需要输入授权密码后才能打开原文。

在档案信息查询利用后，对于浏览时限到期的电子档案（如文件档案借阅）进行权限撤消，实现档案信息的回收。

3.4.3.4 档案输出安全

档案输出的安全是查询利用中需要重点考虑的方面，除了前面提到的操作过程管控外，还应控制有浏览权限的人是否能复制、打印、摘录、传播等，从而保证敏感档案信息不被泄漏。对打印时间，打印次数，打印份数等，都应该进行控制。在档案输出时，可以自动加入水印，防止原文信息的扩散。

对于档案输出中的原文下载，应当控制下载后原文的打开权限，只有有相应身份认证的用户才能打开，并可以控制下载原文的打开设备，如：指定在某台计算机或设备上才能打开。同时，对下载后的原文进行打开次数的控制，屏蔽原文的截屏功能，并做到下载原文超过时限后的自动销毁。同时，实现对用户查询利用过程中输出的数据进行追踪控制，追踪控制的内容包括传输情况、操作行为等。

应当实现终端计算机不留密功能，所有对档案信息管理系统的访问应当指向某一安全终端访问平台，使档案信息不能未经系统许可就直接下载到本地终端上，确保档案信息不被拷贝和泄漏。

3.4.3.5 安全审计分析

档案信息管理系统应当具备对利用过程的记录监控功能，通过安全审计对档案信息的使用过程进行详细的记录，每个审计事件与引起该事件的用户身份相关联，日常对可能有风险的事件行为进行分析查看，发生问题时能够追朔问题的源头。审计记录的内容至少应包括：事件发生的时间（或时间段）、事件发起用户 ID、用户操作的客户端、事件内容、事件的结果，对审计记录数据进行统计、排序、分类、搜索以及分析生成报表的功能，并实现安全可视化，所有的安全行为事件、分析结果等。安全审计功能尽可能有一个统一的界面进行展示，以方便管理。同时，可以自定义安全规则，针对操作行为与规则的匹配度自动进行相应的审计。审计中应包括分析和警告的功能，如一个用户在非工作时间段访问系统，或者在工作时时间段访问非授权的档案信息，系统应予以拒绝并记录在案，并通过警告提示管理员，以便进行跟踪处理。

同时，安全审计应可以对利用者的利用情况进行综合管理，包含利用者信息、利用时间、利用档案信息、利用目的、利用人次、利用效果等，既便于档案馆响应各种各类利用需求，又能够在其中发现在利用过程中可能存在的风险点，提高安全防护水平。

3.4.3.6 人员、场地、设备等的管控

查询利用过程中的安全还涉及对人员、场地、设备等的管控。在档案查询利用场所，一般应限制利用人员携带手机、U 盘、数码相机、笔记本电脑等设备。在查询利用的场地上要有严格的监控措施，避免利用人员不当操作，并记录整个利用过程。同时，不同级别的档案信息利用应实现网络隔离，对查阅利用计算机的输入和输出口（USB、串口、红外、Wifi 等）进行安全管控。同时系统应实现只能在指定专用的查阅利用计算机上进行电子档案的利用，禁止传阅到其他计算机上等功能，保证档案信息查询利用的安全。

3.4.4 信息公布

信息公布，这里指的是档案信息通过编研、出版、展览等方式提供利用，既包括在线利用，也包括离线利用的过程。

3.4.4.1 编研开发

在档案编研开发过程中同样存在着对操作过程的控制和审计。同时，编研过程中会通过复制、剪切、编辑等生成新文件，应当要防止编辑生成的新文件中档案信息外泄。因此，应该对编研开发过程中的档案信息进行加密，避免其被直接复制到本地计算机中。系统应当可以控制目录数据的字段值内容、电子原文的内容等在编研过程中的复制。同时，要严格控制文件的下载权限，避免在编研过程中获取到没有下载权限的重要信息。

在编研成果发布时，可以控制专题发布的目录字段、原文格式、是否加水印、发布的页码、是否需要身份认证才能利用等。对于编研成果的发布情况，也应当专门记录发布日志。

同时，系统要加强编研过程的终端控制。编研人员必须在具有权限的终端计算机上才能进行操作，并且要绑定身份认证信息，防止其他人员通过编研操作获取不应知晓的档案信息。

3.4.4.2 离线利用

在档案信息公布过程中，往往涉及到档案信息的离线利用。这里的离线利用，特指档案信息脱离系统后的各种利用。现实情况下，不管是在档案查询利用还是在信息公布时，都存在着档案信息导出系统提供利用的情况。

离线利用安全保护主要要考虑的是档案信息及其相关的存储介质的加密控制，具体地，应当包括以下几个方面：

（1）事前，设置好身份认证措施，必须要经过身份认证后的用户才能访问离线档案信息，如通过管理手段或与数字证书绑定等，没有插入相应的证书则无法访问；对于某些特别重要的文件，禁止离线查看，必须通过终端不留密的方式在线阅读。

（2）事前，在档案信息导出系统时，应当限制对离线档案信息的访问时间和访问次数，并通过档案信息系统将此属性嵌入到信息内部，做到“阅后即焚”。

（3）事中，为了防止档案信息的复制而导致传播范围扩散的问

题，应当设置对电子档案的副本拷贝无法操作或者结果无效；应当根据权限情况，限制对档案信息中内容的复制，禁止截屏功能，利用电子水印等技术防止拍照；对于档案信息的篡改，要能做到一经篡改便不可使用，或者不可按既定的规则打开，从而使其他使用者可以看出来这是一个被篡改过的文件。

（4）事后，在访问时间或访问次数到达时，能自动销毁离线利用的档案信息；必要时可以对档案信息及其相关的存储介质进行追踪，记录访问和操作情况。

（5）对终端计算机及存储介质进行安全管控，避免造成被病毒感染、木马程序窃取或通过邮件等方式流传到公众网络中。对档案信息存储介质及其相关设备进行标识，严格登记设备台账，并记录设备管理人员以及设备去向，如设备损坏或报废，应由指定的专门机构进行处理。

3.4.5 对外发布

前面提到，档案信息对外发布指两种情况，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系统，向有权限查阅的用户主动的分发共享档案信息。它应当包括以下的功能需求：

（1）事前，应当对档案信息进行分类，按照相应权限进行分发。所有的对外发布请求必须通过审批，并记录在案，可查阅、可审计、可跟踪。

（2）事中，对外发布的档案信息的使用必须经过身份审批，只能由指定的用户打开或调阅；对外发布的档案信息进行硬件绑定，不允许脱离该硬件，即使脱离该硬件也无法访问；对发布所采用的硬件设备进行管控，登记在案；对可能产生泄密的重要行为或异常行为进行告警，如批量外发、尝试非法操作等。

（3）事后，对外发布的档案信息超过指定时间期限或达到指定打开次数，文件自动销毁。

（4）对档案信息网站进行安全加固。为网站安全保护提供统一的策略管理和服务，包括用户操作策略、进程策略、文件密级策略、审计跟踪策略等等。进行网络的隔离，避免由于网络的开放性、互连性等特征而导致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、篡改的问题。实行网站系统管理员、信息安全管理员、信息发布审计员“三员分开”制度，建立操作日志。

（5）对外发布后的档案信息应进行追踪，包括传输路径、利用情况等，并对相关情况进行分析，必要时向系统发送警告信息。

档案信息利用过程中的安全防护是一项整体的工作，因此，要对以上的这些档案信息利用过程中各个环节的功能需求进行统筹考虑和规划，使之在统一的安全管控之下实施，使得安全防护工作成为一个有机的整体，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。

第四章 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实现方式

4.1 常见技术手段介绍

本章讨论提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安全保护功能的具体实现方式，主要从技术层面讨论，也涉及一些管理手段。在讨论整体的实现方式之前，我们先对目前常见的适用于档案信息安全的技术手段进行一个概述，为后续具体的实现提供铺垫。

4.1.1 身份认证技术

档案信息访问控制中最基础也最重要的技术就是身份认证技术。身份认证是在计算机网络或系统中确认操作者身份的过程。身份认证可以基于用户知道的东西、用户拥有的东西或者用户的生物特征。比如要求用户在知道口令、或者拥有数字证书、或者依据系统认可的指纹的条件下，才能访问档案信息系统或者拥有档案信息系统的某些功能。同样，可以在访问集中存放档案信息的存储或者软件系统或者数据库上使用身份认证技术。

（1）口令

口令是最常用的认证方式，在档案信息系统中使用的口令应当有一定的要求，比如长度、大写字母、小写字母、数字、特殊字符混合，不同的系统要求不同的口令，这样才能保证口令不易被破解。口令在

使用上还要注意加密的问题，系统在数据库中存放口令或者在网络访问时传输口令要采用加密的方式，否则就有可能存在黑客在非法获得数据库权限后就知道了全部的用户口令和黑客通过网络窃听获得用户口令的风险。在实际应用中，单纯的口令认证常常不能达到理想的安全。

（2）认证令牌

认证令牌是一种代替口令的较好手段。认证令牌是一种小设备，每次用户输入一个规定的信息，认证令牌就根据规则输出一个口令。这个口令每次都不一样，生成后口令可以使用一段时候之后就失效。使用认证令牌时，每个用户都要有一个认证令牌的小设备，一般在一些安全要求比较高的档案信息系统中可以选择使用。

（3）USBKey 身份认证

基于 USBKey 的身份认证方式是近几年发展起来的一种方便、安全的身份认证技术。它采用软硬件相结合、一次一密的强双因子认证模式，很好地解决了安全性与易用性之间的矛盾。USBKey 是一种 USB 接口的硬件设备，它内置单片机或智能卡芯片，可以存储用户的密钥或数字证书，利用 USBKey 内置的公钥算法实现对用户身份的认证。基于 USBKey 身份认证系统主要有两种应用模式：一是基于冲击/响应的认证模式，二是基于 PKI 体系的认证模式。

（4）证书认证

基于证书认证也是现在较常用的认证，它基于用户的数字证书。数字证书是一个计算机文件，它证明了与公开密钥的关联。在政务网

有个各方信任证书机构发放政务CA证书，在互联网也有商用CA证书。各级国家综合档案馆在其他单位或个人利用电子档案信息时可以要求对方提供它的数字证书，以便档案馆确认对方的真实身份。在安全要求比较高的档案信息系统中，可以要求登录用户使用个人CA证书，确保登录用户没有被假冒，防止非法访问，对用户在系统中的行为进行有效管理。

4.1.2 行为审计技术

行为审计包括对档案数据库的审计、应用行为审计以及服务器和终端的审计，通过详细的审计和分析，可以发现档案信息利用过程中的安全风险和威胁。

（1）档案数据库审计

档案数据库审计能够实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断。档案数据库审计通过对用户访问数据库行为的记录、分析和汇报，用来帮助用户事后生成合规报告，对事故追根溯源，同时加强内外部数据库网络行为记录，提高档案信息利用中的安全。

（2）应用行为审计

应用行为审计主要审计用户对档案信息系统的操作行为。应用行为审计一般要结合应用具体的功能开发，由于在每一种应用的功能模块中都内嵌了相关的审计功能，因而可以实时对系统的行为进行审

计，并通过分析、告警和阻断，维护系统和数据的安全。

（3）服务器和终端审计

服务器和终端的审计包括对重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件，主要包括事件的日期、时间、类型、主体标识、客体标识和结果等。一般服务器和终端的审计可视化程度较差，因此，可以通过专业的软件去获取相关日志，转化成易于查看的图表。

审计虽然属于事后行为，但如能及时发现并阻断，也可以解决许多问题，同时，对于安全事故的分析具有着很重要的参考作用。通过行为审计在各级国家综合档案馆中的应用，可以解决档案信息利用过程中的很多安全问题。

4.1.3 终端安全防护技术

终端安全防护技术主要可以用于实现档案信息在终端上的安全防护。目前常见的技术包括：

（1）硬件设备变化监控技术

当终端计算机添加或删除一个即插即用设备时，将触发系统的设备变更通知消息。通过捕获该消息，来获取 USB 移动存储设备、光驱设备等的接入消息，并与服务端通信验证合法性，不合法设备禁止其接入，从而实现对 USB 移动存储设备和光驱设备的安全管控。

（2）API HOOK 技术

API HOOK 技术是一种用于改变 API 执行结果的技术，可以通过

API HOOK，改变一个系统 API 的原有功能。基本的方法就是通过 HOOK“接触”到需要修改的 API 函数入口点，改变它的地址指向新的自定义的函数。终端安全防护中采用此技术实现强制登录防护端，并阻止用户强制终止防护端进程。

（3）进程识别技术

进程识别技术是采用智能进程特征识别技术对受控进程进行识别的技术。由于它不仅仅依赖应用程序名称，因此，无论如何修改应用程序名，都能被正确的识别，这样就排除了进程名修改后产生的档案信息不能自动加密，以及非法的、伪装的进程对密文进行透明解密等泄密风险。

（4）内核级文件透明加解密技术

在操作系统中，所有的文件系统操作都是向 I/O 管理器提出，I/O 管理器将操作定位到具体某个文件系统来完成。而透明加解密技术平台介于 I/O 管理器和 Windows 文件系统的之间，对于档案信息相关文件的操作者来讲，他们不会感觉到 Windows I/O 及底层发生的一切变化。文件经过 Windows I/O、透明加解密技术平台和 Windows 文件系统的处理，最后存放在磁盘上的文件是经过加密的。同时，加密算法、加密密钥、加密策略是内置在透明加密技术平台中的，由系统管理员集中管理的，文件操作者是无权获取或更改的。

4.2 档案信息利用过程中安全保护的实现方式

根据功能需求方案和常见技术介绍，我们认为，档案信息利用过

程中各个环节的安全保护具有一些共性的特点。因此，要实现档案信息利用过程中安全保护的目标，要从以下几个层面进行防护：

首先，要建立一个通用的基本安全防护，这个基本安全防护贯穿于档案信息利用的每个过程，如：用户认证、权限控制等，属于每个过程都需要的基本防护，并且在整个档案信息利用过程中，要保持这些基本安全防护的一致性。

其次，根据档案收集整理、存储传输、查询利用、信息公布、对外发布等过程的安全保护需求侧重点，我们分别设计了各个过程安全保护实现方式，通过基本安全防护和各流程动态安全保护的联动保护机制，结合成一个有机的整体，建立起主动性、动态性、全过程的安全保护系统。在这当中，为了保证覆盖事前、事中、事后三个阶段，我们将事前安全策略的设定归于基本安全防护，事中的防护我们嵌入到每个具体的过程中，同时，事后的审计和跟踪则跨越了基本安全防护和具体的利用流程。

在档案信息利用过程中安全保护功能的实现，可以内嵌到电子文件与电子档案管理系统中，成为电子文件与电子档案管理系统的内置功能，也可以通过与第三方的安全产品集成来实现，以便在档案信息利用过程中能够应用到相关专业的安全产品，如数据库审计设备、堡垒机等。通过调用安全集成接口，进行相关的交互，使第三方安全产品为整个安全保护功能提供专业化的安全服务，并有效利用现有的档案信息系统在安全方面的投资，节省实施成本。关于安全保护功能的统一策略配置和管控，可以在电子文件与电子档案管理系统的系统管

理模块中统一设置。

具体的实现架构图如下：

4.2.1 基本安全防护

基本安全防护涉及档案信息利用过程的各个环节，为各个环节提供统一的、最基础的安全防护。

4.2.1.1 用户认证

用户认证是安全防护最基础的功能，所有访问档案信息的用户，无论内部用户或者外部用户，都必须先通过身份认证。在不同的应用场景中，可能需要采用不同的用户认证方式，但对每个用户在整个过程中的标识必须是唯一的，这样才能保证权限控制的连续性和准确

性。通过用户认证，实现对利用过程中各类人员身份的识别，从而控制其权限，确保档案信息在适当的范围、适当的时限内传播利用，并防止非法用户登录。

利用档案信息，目前大多数档案馆一般采用用户名+密码认证，为了防止用户身份被冒用，密码应强制有一定的复杂度，如：要求数字、字母和符合三者的组合，如果条件允许建议结合 CA 认证或生物特征认证技术（如指纹、虹膜等）以提升认证强度。在档案信息公布和对外发布利用过程中，除非完全放开权限的用户或数据，否则需要采用用户名密码认证和 USBKey 认证（或 CA 认证、动态口令、生物特征认证技术等）相结合的方式。系统应能在多次输错密码后自动销毁证书，并主动向系统管理员告警，后续用户通过审核手续解锁后才能申请新的证书登录，确保系统的安全性。需要注意的是，为了便于系统间的衔接，应当一开始就设定用户账号创建的策略，使其统一、标准。除此之外，系统还应实现以下的功能：

1. 账户管理

账户管理涉及创建、维护和关闭用户账户。

（1）账户创建。各级国家综合档案馆档案信息利用的用户账户创建须通过已制定的安全策略进行保护，所有新建账户都需要运用统一的安全策略进行创建，拥有高权限的账户被创建时，需经过有关部门审核批准。新建账户的分类及安全级别在创建时即被严格指定。

（2）账户维护。各级国家综合档案馆档案信息利用的账户维护工作，涉及更改账户的权限和特权，在未经授权的情况下，增加或减少

用户权限都会导致严重的后果。因此，对账户的维护过程，应当经过严格的审批过程。

（3）账户关闭。当某个账户不再使用时，应将其用户账户及时禁用并删除，在相应的数据表中将其相关信息进行处理，必要时可对该账户信息进行备份存储。

2. 监控账户和日志

监控档案信息利用的用户账户事件记录与系统日志，有助于将各种利用操作时间线上的任何参考点处的状况拼接在一起。事件记录和系统日志应当能够捕获事件、更改消息以及描述档案信息系统上所发生活动的其他数据，并能够综合使用它们得出需要调查的事件的结论。如：在外部攻击者通过使用某个脆弱服务之后非法获得账户时，我们可以通过事件记录和系统日志了解与这个事件相关的信息。因此，可以在档案馆服务器以及防火墙中设置一定的访问控制机制，并实时记录访问信息，这些日志信息要同时备份到数据服务器中，以防日志被删除。

3.安全保护功能的用户认证

这里指的是安全保护相关功能模块的管理账户认证。基于安全保护功能涉及到系统的安全，因此，应设计独立的用户认证模块，一般只允许系统管理员进行操作，同时，设置安全管理员、安全审计员等角色监控系统管理员的操作行为。系统管理员、安全管理员、安全审计员三员的日志应当是互相独立的。

4.2.1.2 权限控制

档案信息利用过程中的权限控制，需结合权限管理，综合集成身份认证、硬件绑定等多项前沿技术。这里包括对档案信息系统操作、对数据操作和对文档本身操作的权限控制三个部分。

一般对档案信息系统操作的权限控制可以运用信息系统的权限控制功能，通过权限控制功能，对用户可能进行的相关操作进行完整的定义，在定义基础上，设计权限管理系统，对每个用户能操作那些功能进行限定。权限控制时，要考虑细化到那一类的操作，有些操作可以归一个大类，如对某个功能模块的操作，有些必须细到具体的动作，如对截屏操作、下载操作等等较为敏感的操作，这具体在后面的各流程动态安全保护中会具体谈到。

对数据的操作可以运用信息系统的权限控制功能，但是要在对档案数据分类整理好的基础上，系统可以细化到对每个档案条目和数据文件进行操作控制。同时，要考虑到用户可能对数据复制、增加、删除、修改等操作的控制。

对文档本身操作的权限控制，可以直接将权限控制功能内嵌到文档属性中，实现对受控文档的精确权限控制，有效控制使用者对核心文档的阅读、修改、打印、授权、解密等操作权限，从根源上防止文档在使用者之间非法使用而造成档案信息的泄露、篡改等，有效保护各类档案信息的安全。

4.2.1.3 行为审计

行为审计是安全防护很重要的功能，应渗透至档案信息利用过程中的各个环节，可以说，只要有对档案信息操作的地方，就有行为审计。这里的行为审计功能，要实现对档案信息在利用的各个环节的操作进行记录，并通过安全中心的审计分析工具集中对用户行为进行安全分析。通过集中分析，便于找出行为的关联，对危险的操作进行实时报警和阻断，有利于对风险进行预判，有利于动态的档案信息安全防护。

前面提到，行为审计可以大致分为档案数据库行为审计、应用行为审计、服务器和终端审计三个层面。系统应保持整个利用过程的记录，对档案信息的各类利用操作一定要留下痕迹，记录应包括哪个时间、哪个设备的哪个用户已经或试图读取、操作哪些信息等等。应记录系统的安全相关事件，包括系统资源的异常使用、重要系统功能的执行等。具体从功能实现上来说，应该包括以下几点：

1.多层业务关联审计

通过应用层访问和数据库操作请求进行多层业务关联审计，实现对档案信息访问者的完全追溯，包括：操作发生的URL、客户端的IP、请求报文等信息，通过多层业务关联审计更精确地定位事件发生前后所有层面的访问及操作请求，使档案系统管理人员对用户的行为一目了然，真正做到操作行为可监控,违规操作可追溯。

2.细粒度数据库审计

通过对不同档案数据库的SQL语义分析，提取出SQL中相关的要

素（用户、SQL 操作、表、字段、视图、索引、过程、函数等）， 实时监控来自各个层面的所有数据库活动，包括来自应用系统发起的数据库操作请求、来自数据库客户端工具的操作请求以及通过远程登录服务器后的操作请求等。通过远程命令行执行的 SQL 命令也能够被审计与分析，并对违规的操作进行阻断。不仅应对档案数据库操作请求进行实时审计，而且还可对数据库返回结果进行完整的还原和审计，并可以根据返回结果设置审计规则。

3.全方位风险控制

通过档案信息的相关记录进行分析，从而控制风险。可以根据登录用户、源 IP 地址、数据库对象（分为数据库用户、表、字段）、操作时间、SQL 操作命令、返回的记录数或受影响的行数、关联表数量、SQL 执行结果、SQL 执行时长、报文内容的灵活组合等来定义所关心的重要事件和风险事件多形式的实时告警：当检测到可疑操作或违反审计规则的操作时，系统可以通过监控中心告警、短信告警、邮件告警、Syslog 告警等方式通知管理员。

4.2.1.4 安全可视化

安全可视化功能是指将档案信息利用过程中发生的各类安全事件，通过可视化的图表展示出来。通过可视化处理，海量的行为数据转换为可以直观展现的安全信息，以实现对利用过程中安全状况的实时掌握，有效提升档案信息安全防护能力。

系统应统一所有行为的可视化视图，可以按授权查看档案信息的

用户行为、安全风险及威胁。提供的视图应包括仪表盘、趋势图、分布图和各种表格等。系统可以按照不同纬度进行统计分析，证明已经发生了什么以及存在哪些安全风险；并能跟踪行为的横向移动，确定对档案信息的某一个行为的发起者、时间、终端等关键信息。

安全可视化可以应用前端展现技术，使用不同形式的图表进行展现，详细见下表。

名 词	描　　述
line	折线图，堆积折线图，区域图，堆积区域图。
bar	柱形图（纵向），堆积柱形图，条形图（横向），堆积条形图。
scatter	散点图，气泡图。散点图至少需要横纵两个数据，更高维度数据加入时可以映射为颜色或大小，当映射到大小时则为气泡图
k	K 线图，蜡烛图。常用于展现股票交易数据。
pie	饼图，圆环图。饼图支持两种（半径、面积）南丁格尔玫瑰图模式。
radar	雷达图，填充雷达图。高维度数据展现的常用图表。
chord	和弦图。常用于展现关系数据，外层为圆环图，可体现数据占比关系，内层为各个扇形间相互连接的弦，可体现关系数据
force	力导布局图。常用于展现复杂关系网络聚类布局。
map	地图。内置世界地图、中国及中国 34 个省市自治区地图数据、可通过标准 GeoJson 扩展地图类型。支持 svg 扩展类地图应用，如室内地图、运动场、物件构造等。
Heat map	热力图。用于展现密度分布信息，支持与地图、百度地图插件联合使用。
gauge	仪表盘。用于展现关键指标数据，常见于 BI 类系统。
funnel	漏斗图。用于展现数据经过筛选、过滤等流程处理后发生的

	数据变化，常见于BI类系统。
evnetRiver	事件河流图。常用于展示具有时间属性的多个事件，以及事件随时间的演化。
treemap	矩形式树状结构图，简称：矩形树图。用于展示树形数据结构，优势是能最大限度展示节点的尺寸特征。
venn	韦恩图。用于展示集合以及它们的交集。
tree	树图。用于展示树形数据结构各节点的层级关系
Word Cloud	词云。词云是关键词的视觉化描述，用于汇总用户生成的标签或一个网站的文字内容

在实现安全可视化中，一般可以应用JSON数据格式实现后端与前端的数据传输。JSON 可以将JavaScript 对象中表示的一组数据转换为字符串，然后就可以在函数之间轻松地传递这个字符串，或者在异步应用程序中将字符串从 Web 客户机传递给服务器端程序。使用JSON做档案信息安全可视化的数据格式，可以大大提升可视化的灵活性和效率。

4.2.1.5 安全管控

对档案信息利用过程中的安全防护是一项整体的工作，各种安全措施，包括操作控制、行为审计等，都需要在同一的安全管控之下实施，使得安全防护工作成为一个有机的整体。安全管控是指通过统一的安全策略，为档案信息利用过程中的安全控制提供命令、监控和审计，并通过统一界面展示出来，在这里可以定制安全策略，并进行审计、响应、分析等，结合安全可视化，实现可控的、可视的安全。

1. 安全策略

为档案信息各业务环节设置审计、权限及响应的安全管控规则，并具有自我学习功能，可以通过对审计信息的挖掘学习，不断优化完善策略。主要包括以下安全策略：

审计策略：制定各种审计策略，为档案信息的操作提供审计规则和范围。

响应策略：对不同的档案信息的操作行为制定不同级别的响应规则，方便系统进行安全响应。

权限策略：对不同的档案信息制定不同的权限策略，保障正确的人对正确的数据执行正确的操作。权限策略可以由协同档案管理系统，结合用户对特定档案信息的权限进行控制，可以实现用户级、文件级、操作级的权限控制粒度。

2. 安全分析和响应

通过安全策略、安全分析发现档案信息利用中的违规行为或高风险行为时，包括对事件、用户、数据等的风险分析，发现已发生的、正在发生的潜在安全风险和威胁，并预测未知可能存在的风险，由安全响应及时通知相关人员，以降低安全威胁。

实时监控：系统实时监控正在发生的行为，对违规和风险操作实时产生告警信息。

安全告警：提供对档案信息异常操作事件的获取并发出相关的告警信息，通知相关人员（系统管理员等）进行必要的响应。告警方式支持邮件、短信、站内消息等。

联动响应：对预先设定的特定事件，触发安全防护端、安全管控中心以及其他安全防护措施的联动，进行立体式防护。

4.2.1.6 统一加密

整个档案信息利用过程中涉及数据的加密，应实现统一的加密，可以采取以下的加密流程，有效利用现有的密钥体系和加密算法实现档案信息的加密保护：

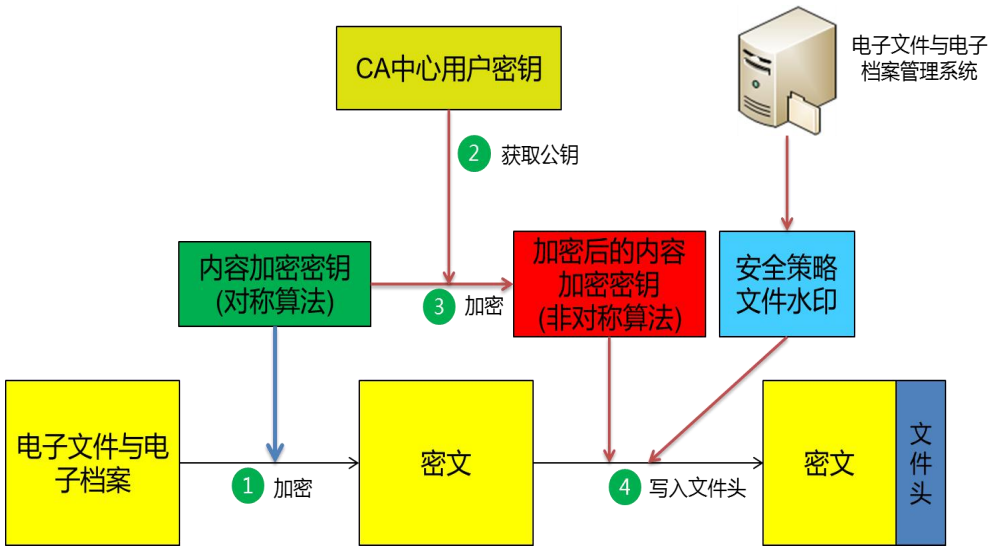


图 4-2 结合现有密钥体系的加密流程

加密过程包括：

①加密：(第一次加密)系统采用获取内容加密密钥采用对称算法对档案信息进行加密。

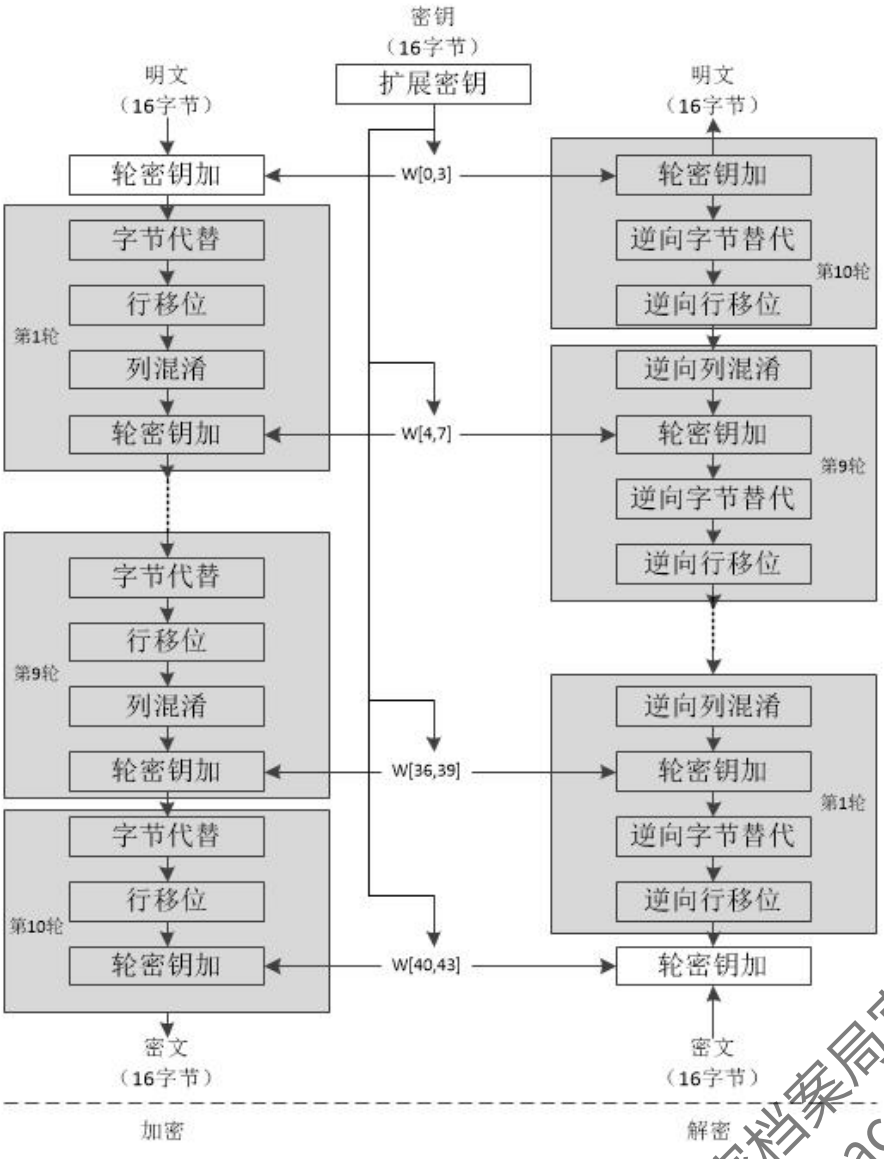
②获取公钥：系统从密钥中心获取当前用户的公钥。

③加密：(第二次加密)采用非对称算法对内容加密密钥进行加密。

④写文件：系统把密文、加密后的密钥信息、策略控制信息、文

件水印信息(文件标识、行为跟踪等)写入文件。

具体的技术实现可以采用标准的、高强度的加密算法进行数据保护，如内容加密算法使用 AES 算法。AES 即高级加密标准（英语：Advanced Encryption Standard），根据使用的密码长度，AES 最常见的有 3 种方案,用以适应不同的场景要求,分别是 AES-128、AES-192 和 AES-256。为保证加密强度，档案信息安全保护系统可以使用 AES-256 实现加密。下图是 AES 加解密流程：



AES 加密过程涉及到 4 种操作：字节替代（SubBytes）、行移位

（ShiftRows）、列混淆（MixColumns）和轮密钥加（AddRoundKey）。解密过程分别为对应的逆操作。由于每一步操作都是可逆的，按照相反的顺序进行解密即可恢复明文。加解密中每轮的密钥分别由初始密钥扩展得到。算法中 16 字节的明文、密文和轮密钥都以一个 4x4 的矩阵表示。

使用 AES-256 高强度算法，可以有效保护档案信息的安全，防止泄密。

4.2.2 收集整理安全保护

4.2.2.1 电子档案接收

为了实现电子档案的接收，并对接收过程中的安全风险进行有效的控制，需要对系统功能进行划分，分为三个模块即管理端、传输端和接收端，每个功能模块分别承担不同的安全职责。

1. 管理端功能

（1）报送单位信息维护

对电子档案报送单位的信息进行维护，报送单位信息至少应包含：单位名称、责任人、联系方式、单位编号等报送单位信息。这些信息的维护包括：新增、删除、编辑、模糊查询、分类查询，汇总报表等功能。这些信息的维护有利于对报送单位信息的认证，从而确认发送的档案信息的有效性。单位信息的编号规则应保持一致，与 CA、身份证等进行绑定，对单位、个人信息的录入一般需要经过审核。

（2）报送单位策略配置和下发

从管理端可对报送单位的资源类型、网络传送参数、报送方式、时间设置、反馈信息、策略同步频率等各类参数进行配置，策略更新后系统支持通过上推和下拉的方式即时更新到传输端。由于一些过程中涉及到大量并发的档案信息的传输，因此要设置好传输策略，避免丢包或传输堵塞等安全问题。

（3）报送单位的添加、安装和卸载

支持对报送单位的传输端软件进行远程维护，包括软件卸载、更新；同时提供软件安装的下载链接。报送单位可登录档案局馆网站，下载传输端软件，在安装或卸载过程中均会与管理端自动确认，管理端可以将软件安装及卸载信息进行集中统一管理。

（4）监控日志审计管理

监控日志主要跟踪报送单位的传送情况，可以根据报送内容、报送单位类别、报送单位、传送数量、传送效果等信息进行有效的查询、汇总、统计、生成报表，并可以根据需要形成月度报表、季度报表、年度统计等报表。

（5）系统参数设置

系统参数主要包括设置通用参数模板以及对网络路由参数、存储目录设置、界面风格、语种、显示方式等参数的设置。

（6）报送单位状态管理

可以实时查询报送单位的传送情况、传送状态，实时显示传送文件、传送流量等信息。

（7）报送单位告警信息

对报送单位的传输端和传送过程以及传送结果中遇到的各类情况实时告警，包括：传输端卸载、连接速率、传送过程网络故障、传送机器对服务器的网络攻击行为、传送文件不完整、传送文件破坏或感染病毒、传输端软件被篡改等信息，根据严重程度做出不同等级的告警，不同的告警信息用不同的颜色予以区分。

（8）传送文件管理和显示

对于传送的电子档案可以进行分类、查询、汇总、删除等操作，并且可以限定接收电子档案的时段、类型、最大限制、命名规则限制等功能。

（9）报送文件统计报告

根据报送的文件情况形成各类统计报表，包括报送文件的报送单位类别、报送单位、大小、类型、数量、报送时间、报送内容等，并生成可视化的视图和统计报表。

（10）审计日志

审计日志对管理员的操作行为进行审计，审计日志包括：管理员配置操作、管理员策略修改、文件删除等操作。审计日志不可以删除，提供审计日志导出功能，可设定保存时间并根据该时间轮巡覆盖。

2. 传输端功能

传输端功能类似数据传输的要求，同时，又包含以下功能实现：

（1）增量传送、差量传送以及压缩传送相结合

对于传输端和接收端的文件，进行差异比较，支持整个目录下文件以及单个文件的增量传送，这样大幅度减少传送量。(如:单个文件

部分修改，则只需要传送修改部分内容)，并且对该差量或增量的数据进行压缩传送，减少传送量。

（2）定时传送

支持定时传送，定时传送可以由管理端统一设置，也可以由传输端根据本单位的具体情况进行设置，可以设置网络忙时段、网络闲时段传送。

（3）自动检测待传送文件列表，管理传送列表

提供查询待传送的文件列表、已传送的文件列表等功能。对于待传送的文件，可以取消传送或暂停传送。

3. 接收端功能

（1）报送用户身份认证

接收端在接收数据前需要对报送的用户进行身份认证，应采用CA等身份统一认证技术。在报送用户信息中可以对传送用户信息进行维护。

（2）多用户并发传输

支持多个用户同时发起的并行传送请求，接收端自动启动各个线程对每个用户的传送请求作单独处理，避免传输过程中堵塞或者丢包的问题。

（3）接收传输文件

支持对传输文件进行格式和内容符合性检查。接收端接到传输文件数据包后，需进行组包、验证、解密、杀毒等接收操作，为了保证数据的安全和规范，也避免病毒或木马进入系统。

（4）元数据检查

按照电子档案元数据方案要求，对照检查电子档案在其文件运行阶段元数据的留存情况。

（5）电子档案准确性检测

检测移交电子档案目录数据是否符合接收要求；校验电子文件是否有电子签章和数字摘要，是否被破坏，内容是否被复制或篡改等要素；自动检测所移交电子档案的内容数据、元数据与目录数据的准确对应。

（6）电子档案完整性检测

按照电子文件归档要求自动检测所移交电子档案内容数据、元数据及相关的文件材料等是否齐全；检测电子档案有无损坏，介质有无损坏，自动生成检测报告，并给出风险提示；对光盘、磁盘、磁带的硬件参数进行检测，给出风险提示。

（7）电子档案可用性检测。

检验电子档案是否可读（包括联系一份文件各个要素的手段是否有效）和是否可靠，载体介质是否完好和兼容，每份所移交电子档案运行环境和格式版本明确，可正常展示，必要时检查是否附带相应的特殊应用软件等等。

（8）电子档案安全性检测

检测所移交的电子档案有无病毒；检测每份所移交的电子档案是否经过安全审核，并按规定做了相应安全处理。

4.2.2.2 数字化加工

数字化加工安全保护的目标就是通过先进的技术手段，全面防护档案数字化和成果报送过程，有效防范人员风险、设备风险、过程风险和报送风险，做到数字化加工工作的事前可防范、事中可控制和事后可审计，从而有效保障电子档案的安全。

1. 全面安全防护

数字化加工安全保护系统针对的是数字化加工整个过程和成果报送过程。横向上，提供档案从实体到数字化到成果报送的全过程防护；纵向上，做到事前防范、事中控制、事后审计的全方位安全防护。事前防范是指通过安全策略的设定，对用户、设备和设备的端口进行细粒度的策略应用和对其安全风险的防范。事中控制是指通过对数字化加工人员的操作控制、对操作系统的进程控制、以及整个过程对档案信息的透明加解密来实现过程中风险的规避、发现和告警。事后审计是指对数字化加工环境中发生的所有行为，包括用户行为、设备行为以及网络行为等，进行审计跟踪，做到事后可以追溯。

2. 人员管控

通过人员管控来规避人员风险，主要包括：

（1）由档案部门人员来担任系统监管员，对现场管理员和操作人员按照工作分工进行权限划分，只有授权的人员才能够正常进入数字化加工环境，及时发现非法接入行为并进行告警；

（2）登记所有数字化加工人员的详细信息，只有登记的加工人员才能够进入到数字化加工环境，系统要对加工人员的所有行为进行

记录和监控。

3. 设备管控

通过设备管控来规避数字化加工设备风险，主要包括：

（1）对用于档案数字化的加工计算机进行登记备案，自动发现非法接入的计算机，并进行告警；

（2）对移动存储设备如U盘、移动硬盘、手机、平板等进行登记和管控，禁止非法接入存储设备，并进行告警；

（3）默认情况下，禁用加工计算机上所有可连通的端口和网络口，如USB、光驱、Wifi、串口、蓝牙等。如需开通，必须通过管理员的认可，并进行记录。

4. 过程管控

通过过程管控来规避数字化加工过程的风险，主要包括：

（1）数字化成果文件在扫描生成时自动进行加密，并且整个数字化过程全程保持加密状态；

（2）采用透明加密技术，数字化加工环境内信任的程序在操作加密文件时自动解密，不对数字化加工人员的操作习惯和工作效率造成影响；

（3）每个加密的数字化成果文件都带有文档标识，包括档案馆名、操作人员、操作时间等信息；

（4）对数字化加工人员何时何地登录数字化系统，以及对数字化成果文件使用过程的操作行为进行记录，便于跟踪；

（5）对数字化加工过程正在发生的行为进行监控，对非法设备

接入、非法操作行为等进行实时告警。

5. 报送管控

通过报送管控来规避报送风险，主要包括：

（1）数字化成果文件在导出到移动存储的整个过程，均存于加密状态，即使移动存储丢失，别人也无法解密；

（2）导出的数字化成果文件只有在监管员的电脑上，利用专用的解密工具和 KEY 才能解密，进行成果文件的挂接，实现档案信息安全保护的完整闭环。

4.2.2.3 数据整理

档案数据整理首先需要建立数据整理的规范和标准流程，按照规范流程进行整理，具体可以参考以下标准和规范：

TA/T22-2000　归档文件整理规则

GB2808-81　全数字式日期表示法

GB3469-83　文献类型与文献载体代码

GB7156-87　文献保密等级代码

GB/T15418-94　档案分类标引规则

DA/T18-1999　档案著录规则

DA/T19-1999　档案主题标引规则

DA/T13-94　档号编制规则

通过数据整理，实现档案数据在层级上的有序化管理，功能包括：

（1）分类管理

能够维护所有档案文件与其所属案卷、类、分类方案的关联，支持把案卷、文件重新定位到分类方案中的不同位置，并保证复合文件和组合文件中的关联保持不变。支持对文件重新分类，并输入重新分类的原因，且作为元数据记入审计跟踪日志。允许标记某类目为关闭状态，防止新类、新案卷或者新文件增加到该类。

（2）案卷管理

可依照规则支持自动或由授权用户为新创建的档案案卷设置唯一标识符与分类代码。支持授权用户根据需要对案卷进行子卷划分，并提供子卷管理。可以对案卷（子卷）设置开放/关闭标记，当案卷关闭之后，确保无法再向该案卷中添加新的文件或者细分新的子卷。可以根据特定的规则关闭或打开案卷，允许打开已关闭的案卷，添加文件后再次将其关闭。在工作结束后，可以手工关闭打开的案卷；在授权用户离线后，任何临时打开的案卷都被自动关闭。

授权用户可以增加、删除、移动、合并、拆分案卷或者对案卷进行重新归类，并能够对案卷的元数据进行自动或者手动调整。可不限制分配到类目的案卷数量，也支持授权用户为类或案卷按照一定规则设定数量限制。支持文件管理员或授权用户对案卷的元数据进行添加、删除和修改。能够显示所有或者特定类、案卷所对应的保管期限。当案卷或者文件从原类目中移动到其他类目时，可允许自动用新类的保管期限代替旧类的保管期限，同时也允许文件管理员或者授权用户手动更改保管期限。

（3）规则管理

可以根据标准定义档案数据整理的规则，自动对授权用户的整理行为进行校验，对于用户不符合系统设定标准的整理操作，予以警告或禁止。在事后保存整理记录，同时对记录进行审计分析。

4.2.3 存储传输安全保护

4.2.3.1 数据传输

在档案信息传输过程中为了保证真实性和安全性，需要对传输过程、文件属性等做严格的安全控制。

（1）大文件自动并发传输、断点续传

由于网络带宽和网络稳定性的问题，大文件传输过程经常由于耗时过长或网络中断传输不成功，由于电子档案数量大、视频文件容量大，因此可以在系统设计时采用大文件的分块传输、多个大文件并发传输的技术。对文件分包传送的时候，每个传送包形成校验码，一旦发现故障则进行数据包重新传送，确保验证无误，并支持传送文件断点续传，在接收端进行自动重新组合，确保档案信息传输利用时的高效和可靠。

（2）区块压缩传输

在档案信息发送端与接收端可以利用 zlib 进行区块间压缩和解压缩，增加网络带宽的利用率，提高传输效率。

（3）数据传输加密

档案信息传输过程中的加密可以采用 SSL 传输加密协议。

通过 SSL 协议指定一种在应用程序协议和 TCP/IP 协议之间提供

数据安全性分层的机制，为 TCP/IP 连接提供数据加密、服务器认证、消息完整性以及可选的客户机认证，以此提高应用程序之间数据的安全性，对传送的数据进行加密和隐藏，确保数据在传送中不被窜改、窃听和伪造实现数据的完整性。

传输通道的安全可以采用 VPN，采用数据加密，应用安全协议，应用信息隐藏技术、水印技术等等来实现。一种是建立秘密的传输通道，非授权无法访问传输通道里的档案信息；一种是对档案信息进行加密处理，即使获得信息也无法知道信息的真正内容。传输通道安全要实现以下的功能：建立安全的访问路径，防止档案信息被盗取、破坏、篡改；在通信双方建立连接之前，利用密码技术进行会话初始化验证；在通信过程中，应对整个报文或会话过程进行加密；通信双方应约定密码算法，计算通信数据报文的报文验证码，在进行通信时，双方根据校验码判断对方报文的有效性，从而确定档案信息的完整性；采用网络层地址与数据链路层地址绑定措施，防止地址欺骗；对传输的档案信息进行检查，防止恶意代码的接收；对档案信息的传输有日志记录。

4.2.3.2 数据存储

采用集中式的存储方案，为档案数据提供稳定、安全、高速、可靠、易扩展的存储空间，使档案存储系统成为档案信息资源整合、共享和优化配置的先进技术手段和载体；成为一个真正的数据中心，实现档案信息共享和增值服务。