现代计算机技术与应用
2022 年 8 月第 4 卷第 3 期

浅析电子文档的信息安全

傅婷婷

江汉大学，武汉

摘　要 | 分析了电子文档的特点，从访问控制、信息加密和数字签名等方面论述了加强电子文档的信息安全的技术措施，并讨论了维护电子文档信息安全的管理措施。

关键词 | 电子文档；信息安全；安全技术

1　电子文档信息安全的内涵

信息安全是信息化时代人们广泛关注的问题。给信息安全下一个简单的通俗化定义，就是：使信息不受威胁或危险。而这里所说的信息安全，是一个特定的专业化概念，国际标准化组把它定义为：“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和显露”。

在传统空间中，由于空间的相对狭隘，信息安全主要是在小范围的保密问题。但随着计算机的使用和网络的兴起，信息被放置在无数人共同享有的平台上，信息安全问题不仅仅是在更大范围的保密（秘密、不泄露）的问题，它还包括保证信息的可靠性、可用性、可控性、完整性和不可抵赖

作者简介：傅婷婷，江汉大学助教。
文章引用：傅婷婷. 浅析电子文档的信息安全［J］. 现代计算机技术与应用，2022，4（3）：81-88.
https://doi.org/10.35534/mcta.0403012c

性等。广义说来，在信息存在和流通的任何一个环节上都有可能存在信息安全问题。

从总体上来说，电子文档信息安全与信息安全的内容基本一致。具体而言，电子文档信息安全主要包括四个方面的内容：（1）实体安全。实体安全是指保护计算机设备、设施（含网络）以及其它媒体免遭地震、水灾、火灾、有害气体和其它环境事故如电磁污染等破坏的措施、过程；（2）运行安全。运行安全是指为保障系统功能的安全实现，提供一整套安全措施（如身份验证、审计跟踪、备份与恢复、应急措施等）来保护信息处理过程的安全；（3）信息安全。信息安全是指防止信息资源被故意地或偶然地非授权泄露、更改、破坏或使信息被非法系统辨识、控制和否认。即确保信息的完整性、保密性、可用性和可控性；（4）管理安全。管理安全是指有关的法律法令和规章制度以及安全管理手段，确保系统安全生存和运营。

2　电子文档的自身特点

电子文档区别于印刷品文档主要有以下四个特点：容易修改，容易删除，容易复制，容易损坏。

（1）容易修改

这是电子文档区别于传统的印刷文档的一个重要标志。印刷文档与手写文档都有一个共同的不足：一旦印刷好或者写好就难于修改，这个特点在某些时候是好的，比如人们经常说的“白纸黑字”就非常能够体现这个特点；但是它的优点也正好是他的缺点，人们在处理很多文字与图形图像信息的时候，经常需要对处理的内容进行修改，以满足不同的需要，这时电子文档就表现出了它的优点。正是由于电子文档容易修改的特点，如果不能很好地保护，就可能受到非法的修改，不管这种修改是有意还是无意的，都会给文档所有者带来一定程度的损失，这时候它又变成一个缺点。

（2）容易删除

对传统方式的文档进行删除基本上是不现实的，只可能对信息的载体印刷品进行毁坏。由于印刷品一般都通过档案室与文件柜等工具来进行保护，相对

来说不容易被一般的人接触，所以也就不容易被破坏，有较好的安全性。但是对于电子文档，其删除是非常方便的，只需要有修改文件的操作权限（这个权限往往可以通过合法的与不合法的手段获得），然后点击鼠标或者通过键盘就可以删除文件。一般情况下，事后也没有任何的证据可以说明文件丢失的时间与原因。正是这样的特点，如果被人利用，进行恶意的破坏活动，可能会给电子文档的所有者造成无可挽回的损失。

（3）容易复制

传统方式的文档进行复制往往需要一些辅助的材料与机器，如复印纸、复印机等相关资料。但电子文档不需要，这是电子文档的又一个优点，也是一个缺点。优点是通过复制，人们可以非常方便地进行信息共享。但是，当文件是个人隐私或者商业秘密的时候往往不希望别人看见，这个时候如果被别人复制，造成个人隐私暴露或者商业信息泄密，都是文档所有者所不愿意看到的，这里需要解决的就是对文件的保密。正是由于它自身的这些特点，电子文档的安全问题就成了一个非常值得关注的话题。如果我们不作任何处理，等到出现问题以后再后悔就来不及了。

（4）容易损坏

文件损坏的原因主要有硬件损坏，人为破坏（有意或者无意），病毒破坏，人力无法抗拒的因素（火灾，地震等），就文件损坏原因的调查中，人为破坏占了 80%，其余的 20% 文件损坏是因为其它的各种因素。对于人为破坏，我们必须采取积极的措施来加以防范，不然很可能会因为疏忽而造成巨大的损失；对人为破坏以外的情况，一个比较有效的措施就是做好备份。

3　加强电子文档信息安全的技术措施

先进的科学技术是保证电子文档信息安全的重心所在。信息安全技术包括：密码技术、鉴别技术、访问控制技术、信息流控制技术、数据保护技术、软件保护技术、病毒检测及清除技术、内容分类识别和过滤技术、网络隐患扫描技术、信息泄漏防护技术、系统安全监测报警与审计技术等。加强电子文档信息安全的技术措施如下。

https://doi.org/10.35534/mcta.0403012c

（1）访问控制

是网络环境下电子文档安全防范和保护的主要措施和手段。它的主要任务是保证包括电子文档信息在内的网络资源不被非法访问和非法使用，具体措施包括：第一，入网访问控制。它控制哪些用户能够登录到服务器并获取网络资源，控制授权用户的访问时间和准许他们在哪个网站入网。有了这道关卡，只有网络合法用户才能进入电子文档信息网站，获取相关文档信息。第二，权限控制。它控制用户允许访问哪些目录、子目录、文件和其他资源；指定用户对这些文件、目录、设备能够执行哪些操作，如只读、改写、创建、删除、查找、存取控制等，而最基本的控制是防止电子文档的拷贝、篡改和打印。第三，防火墙控制。它是用以防止网络中的黑客访问某个机构网络的屏障，也可称之为控制进与出两个方向通讯的门槛，既可以阻止对本机构信息资源的非法访问，又可以阻止机要信息、专利信息从该机构的网络上非法输出。目前的防火墙主要有包过滤、代理、双穴主机防火墙 3 种类型，分别用于不同的网络层来执行安全控制功能。

（2）信息加密

信息加密的目的是保护网内的数据、文件、口令和控制信息的传输，确保不宜公开的电子文档的非公开性。在多数情况下，信息加密是保证电子文档机密性的唯一方法。信息加密过程是由多种多样的加密算法来实施的，通常将其分为常规密码算法和公钥密码算法两大类。在实际应用中，人们常常将常规密码和公钥密码结合在一起使用，比如，电子文档的加密技术就是将两者结合使用的，即发方使用收方的公开密钥发文，收方只用自己知道的密钥解密。由于加密和解密使用不同的密钥，第三者很难从中破解原文的内容，从而确保传输中的电子文档的安全。目前，网上电子文档信息可采用异步数据加密机进行加密处理或使用阿帕比系统（包括数据转换软件、安全文档软件平台、阅读软件 3 个子系统）对用户进行阅读、打印、复制设定控制。

（3）数字签名

数字签名是用来确保电子文档的真实性和进行身份验证，以此确认其内容是否被篡改或伪造。电子文档的签名技术一般包括证书式和手写式数字签名两

种方式。比较两者的优劣，笔者更倾向于手写式数字签名方式。因为手写式数字签名是作者使用光笔在计算机屏幕上签名，或使用一种压敏笔在手写输入板上签名，显示出来的“笔迹”如同在纸质文件上的签名一样，这种“笔迹”是作者以外的人很难模仿的。而证书式数字签名需要向专门的技术管理机构（类似于身份确认的公证机构）登记注册，手续繁琐，没有作者手写签名来得直接和直观。当然，手写签名的“笔迹”也有可能被拷贝下来，然后被不留痕迹的转“签”到其他文件上，造成以假乱真的效果，这就要借助其他安全控制技术，如加密、防伪、真迹鉴定等技术结合使用。

（4）防写措施

防写措施即电子文档设置为“只读”状态，在这种状态下，用户只能从计算机上读取信息，而不能对其做任何修改或复制和打印。如目前网络上的 PDF 格式文件，就是只能供网络上的合法用户阅读，而不能修改和复制，除非另外再下载一个软件，对这种格式的文件进行解读，才能进行复制、打印等操作。此外，外存储器中的只读性光盘（CD-ROM）和一次写入式光盘（WROM）等不可逆式记录介质则可以有效防止用户更改电子文档内容，确保电子文档的真实性。

（5）信息备份与恢复

这是一种防止电子文档信息丢失和失真的补救措施。由于网络的不安全性，导致电子文档信息易丢失或失真，给信息安全带来严重威胁。尽管可以采取各种各样的技术和方法来保证网络的安全，但客观地说，任何一个网络都不能确保万无一失，信息丢失和失真的现象难免发生。如果建立备份与恢复系统，即使信息一旦丢失和失真，也能够做到有备无患，只要启动该系统，丢失或失真的信息就会重新恢复原来的面貌。

4　保证电子文档信息安全的管理措施

电子文件形成、处理、收集、积累、整理、归档、保管和利用等环节，都有信息更改、丢失的可能性，建立并执行一整套科学、合理、严密的管理制度，从每一个环节堵塞信息失真的隐患，对于维护电子文件的原始性、真实性十分

https://doi.org/10.35534/mcta.0403012c

重要。维护电子文件真实性的管理措施涉及从电子文件形成、处理、收集、积累、整理、归档，到电子档案的保管、利用的全过程，可以称之为“电子文件全过程管理”。电子文件的管理不仅注重每个阶段的结果，也要重视每项工作的具体过程，并把这些过程一一记录下来。其中有关维护其信息安全方面的主要措施有以下几个方面。

（1）电子文件的制作过程要责任分明。制作人员应该对其制作的文件负有全责，在合作制作的文件或大型设计项目中，要注意划清参与人员的责任范围。一般来说，不相关人员不能进入其他人的责任范围，需要时可以允许用只读形式调阅，以防由于误操作、有意删改等原因造成文件信息的改变。

（2）电子文件形成后应及时进行积累，以防在分散状态下发生信息损失和变动。机关办公活动中形成的公文性电子文件一经定稿就不得进行任何修改，CAD 电子文件的更改要经过必要的批准手续。收集积累过程中的一切变更都应记录在案。对收集积累起来的电子文件要有备份。

（3）建立和执行科学的归档制度。归档时应对电子文件进行全面、认真的检查，在内容方面检查归档的电子文件是否齐全完整，真实可靠；相应的机读目录、伺服软件、其它说明是否一同归档；归档的电子文件是否最终稿本，CAD 电子文件是否反映产品定型技术状态的版本或本阶段产品技术状态的最终版本；电子文件与相应的纸质或其它载体文件的内容及相关说明是否一致，软件产品的源程序与文本是否一致等。在技术方面应检查归档电子文件载体的物理状态，有无病毒，读出信息的准确性等。

（4）建立和执行严格的保管制度。归档电子文件应使用光盘作为存储介质，对所有归档的电子文件应作写保护处理，使之置于只读状态。在对电子文件进行整理和因软硬件平台发生改变而对电子文件实行格式转换时，要特别注意防止转换过程中的信息失真。对电子文件要定期进行安全性、有效性检查，发现载体或信息有损伤时，及时采取维护措施，进行修复或拷贝。

（5）加强对电子文件利用活动的管理。电子文件入库载体不得外借，只能以拷贝的形式提供利用。对电子文件的利用实行用权限控制，防止无关人员对电子文件系统的非法访问，防止利用过程中的泄密和损伤信息。

（6）建立电子文件管理的记录系统。电子文件形成后因载体转换和格式转换而不断改变自身的存在形式，如果没有相关信息可以证实文件的内容没有发生任何变化，人们是无法确认它的真实性。因此，应该为每一份电子文件建立必要的记录，记载文件的形成、管理和使用情况，用这些记录来证实电子文件内容的真实性。

国际档案理事会电子文件委员会制订的《电子文件管理指南》中指出，有两类相关信息应当记录和保存。一类是“元数据”，即关于电子文件的技术数据。元数据有助于说明电子文件的内容、结构和上下文关系。另一类是“背景信息”，即关于电子文件业务和行政背景方面的数据。背景信息有助于说明文件的真实性，并能帮助文件使用者理解文件的内容。

记录系统应该具有实时记录的功能，随时将需要保留的信息记录下来。由于这种“跟踪记录”具有原始性，它可以成为证实电子文件真实可靠的有效依据。对于从收集积累阶段就在网络系统上运行的电子文件，可通过自动记录系统记录有关信息；对于以介质方式收集积累的电子文件，还要辅之以必要的人工记录。

参考文献

[1] 陈运．信息安全概要 [J]．数据通信，2001（3）：29–31.
[2] 闫志敏．信息安全的内容和实现 [J]．电脑知识与技术，2002（1）：34–35.
[3] 吕诚昭．信息安全管理的有关问题研究 [J]．电信科学，2000（3）：22–26.

https://doi.org/10.35534/mcta.0403012c

Analysis of Information Security of Electronic Documents

Fu Tingting

Jianghan University, Wuhan

Abstract: This paper analyzes the characteristics of electronic documents, discusses the technical measures to strengthen the information security of electronic documents from the aspects of access control, information encryption and digital signature, and discusses the management measures to maintain the information security of electronic documents.

Key words: Electronic document; Information security; Security technology