电子文件证据性概念模型研究

许晓彤

【摘　　要】本文对电子文件“四性”与电子证据“三性”进行系统分析与映射，深入探讨上述概念在文件管理语境和证据法学语境中的内涵与外延、差异与关联，在对概念进行拆解与重塑的基础上构建了电子文件证据性概念模型。该模型包含对应电子证据“三性”的三个圈层，以及真实性、可靠性、完好性、齐全性、可用性、安全性、保密性、合法合规性八项属性。

【关 键 词】电子文件；证据性；电子证据；概念模型；文件管理

【作者简介】许晓彤，山东大学历史文化学院。

【原文出处】《档案管理》（郑州），2021.2.27～31

【基金项目】本文系山东大学基本科研业务费专项资金资助项目“单轨制背景下的电子文件证据效力保障体系构建研究”(2020GN056)的阶段性成果。

本文基于长期保存目的，选取了三种具有代表性的数字资源存储方式，即本地光盘存储、本地服务器存储与云存储，以成本核算普遍使用的方法——会计品种法为依据，分析不同的存储方式对数字保存成本所产生的影响并总结了不同存储方式的适用性。

1 研究背景与研究现状

作为社会生活中直接形成的原始记录，凭证价值是档案资源区别于其他资料的最重要特征，[1]用作司法证据时亦具备证明力优势。

传统纸质环境中，2001年颁布的《最高人民法院关于民事诉讼证据的若干规定》(以下简称《民诉证据规定》)与2002年颁布的《最高人民法院关于行政诉讼证据若干问题的规定》均明确指出档案材料作为书证时证明力一般大于其他书证、视听资料和证人证言。随着技术的发展，学界与业界关于数字环境中的档案材料，即电子文件是否拥有纸质文件同等的凭证价值各执一词、讨论频繁。

2004年，《中华人民共和国电子签名法》(以下简称《电子签名法》)首次肯定了电子文件的证据资格。直至2019年，《民诉证据规定》再次修正，正面指出以档案管理方式保存的电子证据可在无反驳证据的情况下认定真实性。

近二十年中，司法界对电子文件证据资格与证据价值逐步认可。与此同时，文件与档案管理领域的“回应”亦令人振奋，2019年的第716号国务院令《国务院关于在线政务服务的若干规定》明确肯定了单套制归档；2020年最新修订的《中华人民共和国档案法》(以下简称《档案法》)中也明确规定“电子档案与传统载体档案具有同等效力”。

随着电子文件作为证据的可采性障碍逐渐消除，电子文件符合何种要求才能最大限度地确保其证据效力成为档案界的关注重点。

对于不具实体特征、非人工可识读、信息易删改、载体可分离的电子文件而言，[2]“四性”则成为判断其档案身份的最重要标识。基于此，国内外学者纷纷开展了跨学科理论研究，探索电子文件与电子证据属性的关联，实现文件与档案管理与证据法学的理论衔接。

国外方面，露茜安娜·杜兰蒂(Luciana Duranti)考察了数字取证(Digital Forensics)学科中对于“可信(Trustworthiness)”的定义与要求，指出真实性、可靠性与准确性是可信文件的属性，并将上述属性在档案学与数字取证学中的定义进行了比较分析[3]；科

琳·罗杰斯(Corinne Rogers)则分别从文件管理与证据法学的视角对比了真实性的概念,探究了真实性的影响因素,[4]等等。

国内方面,张宁结合证据的真实性定义,解析了电子文件真实性的内涵[5];崔屏在电子文件"四性"的基础上加入证据的合法性,使其共同构成电子文件凭证性概念模型[6];刘越男将电子文件的"四性"与电子证据"三性"进行了比较,提出可将电子文件的完整性分解为要素齐全的"齐全性"和未被非法改动的"完整性";将证据的真实性分解为形式真实的"真实性"与内容真实的"可靠性",以实现两个领域间更顺畅的衔接[7][8][9]等等。

2 电子文件的"四性"与"新四性"

文件与档案管理领域普遍认可电子文件的"四性"一般为ISO 15489-1:2001《信息与文献 文件管理 第1部分:通则》[10](同等国标采标GB/T 26162.1-2010)中列举的真实性(Authenticity)、可靠性(Reliability)、完整性(Integrity)与可用性(Usability),[11]我国GB/T 18894-2016《电子文件归档与电子档案管理规范》[12]亦遵循这一划分方式。但在我国的电子文件管理实践中,还较为强调"安全性"(Security)这一特征,逐渐形成了真实性、完整性、可用性、安全性的"新四性"。

中办国办厅字[2009]39号《电子文件管理暂行办法》、DA/T 70-2018《文书类电子档案检测一般要求》[13]即采取这一定义。为求全面,本文将综合分析上述五项属性的内涵与关系。

2.1 电子文件的真实性。"真实性"是电子文件管理领域中出现频率最高的术语之一,是传统环境中"原始性"概念在数字时代的发展。[14]档案界对真实性的定义大致有三类表述方式:

第一类强调"目的、人员、时间三个关键条件一致",ISO 15489(GB/T 26162.1-2010)对此进行了具体描述。第二类强调"内容、背景、结构三项基本要素不变更",如GB 18894-2016和DA/T-70-2018规定电子文件和电子档案的真实性为"内容、逻辑结构、形成背景与形成时原始情况相一致的性质"。第三类则是将前两者的表述方式结合起来,同时强调关键条件与基本要素的前后一致,如DA/T58-2014《电子档案管理基本术语》。[15]

综合分析发现,上述定义均是将文件的现有状态与其形成之时的状态进行比对,确认一致后即确定真实性。由此可知,真实性是一种是否判断,是指一种"形式上的真实"[16],这与日常生活中客观真实认识相似,这个层面的真实,还需要引出下一个属性——可靠性。值得注意的是,"形式"可与"内容"相对,亦可与"实质"相对,二者释义不同。此处所指的"形式"是与"内容"相对的"形式"。

2.2 电子文件的可靠性。关于可靠性的定义,各类标准规范中的描述都趋向一致。ISO 15489认为:"一份可靠的文件是指文件的内容可信,可以充分、准确反映其所证明的事物、活动或事实"。GB 18894-2016和DA/T 58-2014均指明可靠性为"电子文件、电子档案的内容完全和正确地表达其所反映的事物、活动或事实的性质"。

上述定义有两个重点:一是可靠性是描述文件内容的属性;二是文件内容只有达到可信,并充分、准确、完全和正确地反映事物、活动或事实。

这与真实性不同,可靠性的实现需要文件内容具备充分、正确地反映客观事实的能力,且可靠性随着文件内容反映客观事实的能力而变动,越能体现客观事实,可靠性越大。张宁亦指出,真实性是一种"确真"的考量,而可靠性是一种"本真"的反映。[17]

可靠性在实践工作中极难检测与衡量,往往涉及各类环境的交错与人员的交互,难以设定一套统一的标准用于判断所有文件反映的内容与已发生事实是否吻合。因此,对于文件可靠性的确认常依赖于对文件真实性的判断,借助"形式上的真实"确认"内容上的真实"。

2.3 电子文件的完整性。虽然ISO15489中完整性所对应的英文译法为"Integrity",但在档案学的语境中,完整性可进一步细分,既有档案学的经典释义"Completeness"(齐全),也有信息安全领域的"Integrity"(完整)。[18]

关于"完整性",首先侧重于"齐全",其次侧重于"完好"。GB/T 20984-2007《信息安全技术 信息安全风险评估规范》中对此进行了具体表述。[19]

2.4 电子文件的可用性。各项国际、国内标准对可用性定义几乎一致,均指文件能够被定位、查找、

检索、呈现或理解。可见，电子文件可用性建立在真实性和完整性基础上。

2.5 电子文件的安全性。安全是档案工作的底线，是档案事业的根基。[20]《电子文件管理暂行办法》和DA/T 70-2018中均将安全性作为电子文件管理的要求与属性。根据DA/T 70-2018的定义，安全性指管理过程可控、数据存储可靠、未被破坏、未被非法访问的性质。

这样来看，安全性与真实性、完整性的概念似乎有所交叉。细究相关定义，DA/T 58-2014中的安全性检验是指“通过管理和技术措施识别电子档案潜在安全性缺陷的过程”，DA/T 70-2018进一步将其分解为对归档信息、归档载体和归档过程的安全性检测。

据此，不难解释为何安全性会与其他属性产生交叉：真实性、完整性以及可用性都是用于描述文件本身的属性，而安全性是针对文件管理的环境、文件载体、文件管理操作过程等相关因素提出的属性。

严格意义上说，安全性与其他三个属性的划分维度并不相同，其提出是源于对电子文件管理安全问题的重视。

3 电子证据“三性”

3.1 电子证据的真实性。证据的“真实性”在传统证据法学中称“客观性”。一是指证据本身具备客观存在的形式；二是指证据的内容是对案件有关事实的反映。[21]

但客观一词容易产生歧义，如取“在意识之外，不依赖精神而存在的，不依人的意志为转移”之意，那所有证据都具有一定客观性；如取“按事物本来面目去考察，与一切个人感情、偏见或意见都无关”之意，则部分证据难免具有一定主观性。[22]由此，法律文件中已呈现出用“真实性”取代“客观性”的趋势。

如前所述，证据的真实性既包括形式上的真实性，又要具备内容上的真实性，此处的语境中，“形式上的真实”与“内容上的真实”相对。

但从整体上说，证据的真实性强调的是一种法律上的真实性，而非客观真实，其本质也是一种“形式真实”，此处“形式真实”又与“实质真实”相对。

为避免歧义并与电子文件管理领域习惯表述保持统一，下文所提及的“形式真实”均指前一种意思。

法律法规中对证据真实性的审查判断规定也体现对证据形式和内容的要求，如《最高人民法院关于适用〈中华人民共和国刑事诉讼法〉的解释》第93条第3款指出，应当重点审查“电子数据内容是否真实，有无删除、修改、增加等情形”，同时提及对内容真实与形式真实的要求。

此外，在电子证据真实性的审查判断中，完整性和可靠性也常作为衡量证据真实性的二级属性。如《电子签名法》第8条规定对数据电文真实性的审查一连用了三个可靠性——生成、储存或者传递数据电文方法的可靠性、保持内容完整性方法的可靠性、用以鉴别发件人方法的可靠性；两院一部《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》第22条第5款中规定了电子数据的真实性需要审查其完整性。

GB/T 22080-2008《信息技术 安全技术 信息安全管理体系》中认为完整性即能“保证资产的准确与完整”的品质，这恰说明了完整性可以作为考察真实性的一个侧面，[23]可知电子数据的完整性倾向于信息安全中“Integrity”的含义，指不被篡改或破坏的品质。

3.2 电子证据的关联性。关联性，亦作相关性，指证据必须与待证明的案件事实或其他争议事实具有一定联系。[24]在我国，对关联性的要求强调必须对证明案件事实具有实质性意义。

相比于其他的证据属性，关联性较容易判断与识别。但人们对证据关联性的认识一般受到科学技术发展水平的影响。如DNA技术使许多不足以成为证据的材料发挥了证据作用，一份电子证据的内容本身或许对案件事实没有直接证明关系，但通过对日志文件的提取审查，其时间线索可能会对案件事实起到间接证明作用等。

3.3 电子证据的合法性。证据的合法性与证据资格相关，是证据能够上法庭的“门槛”。证据合法性的判断要点在于调查主体、证据形式与收集提取须符合相关法律规定，[25]此处的重点在于强调电子证据不能是非法获取的，否则将予以排除。此外，实施取证之前，如果电子证据通过非核正程序(Ap-

proved Process)和非法软件生成,则也被看作不具有合法性。[26]

综上可知,真实性、关联性是对证据本身提出的要求,可视为证据的本质属性;即便证据的合法性有瑕疵,该证据所具有的真实性和关联性也使其拥有反映待证事实的能力。而合法性更关注证据获取的手段和程序,是为证据的外在附加属性。[27]

4 电子文件与电子证据属性的映射与对接分析

通过对电子文件"四性"与电子证据"三性"的梳理,可知真实性、完整性等在档案学语境和证据法学语境中具有不同内涵与外延,但也存在一定关联。

在此基础上,本文试图对"三性"与"四性"进行映射与对接,实现电子文件与电子证据属性的衔接。

如图1与表1所示,电子证据的真实性包含形式的真实和内容的真实,强调其能够还原客观真实的能力,同时以完整性、可靠性等概念作为真实性的审查要点。

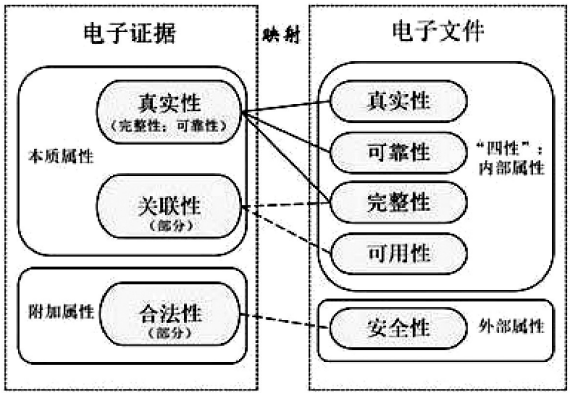

图1 电子文件与电子证据属性映射图

表1 电子文件与电子证据属性概念对接表

电子证据		电子文件		
真实性	以完整性和可靠性作为审查要点	真实性	形式的真实——目的、人员、时间三大关键条件与内容、背景、结构三大要素与形成时一致	
		可靠性	内容的真实——文件内容可信,并充分、准确、完全和正确地反映事物、活动与事实	
		完整性 可用性	完整性 1Integrity-完好	侧重信息安全领域定义方式
关联性	与待证事实有实质性联系		完整性 2Completeness-齐全(部分对接)	侧重档案学经典定义方式
			(部分对接)直接表明文件与形成它的业务活动和事务过程	
合法性	过程与方法符合规定	安全性	(部分对接)系统合法、环境可靠	

该属性映射到电子文件中,对应着真实性、可靠性、完整性三个概念。电子文件的真实性对应电子证据真实性中的形式真实,可靠性对应真实性中的内容真实、电子文件完整性取完好无损,未被篡改、破坏之意时,与电子证据真实性概念中下属的完整性定义一致。

由上可知,电子文件完全具备电子证据最核心的真实性要求,这从侧面印证了司法对档案管理工作证明力优势的认可。

电子证据的关联性表示与待证事实有实质性的联系,其部分内涵与电子文件的完整性与可用性相对应。当电子文件本身的内容、背景、结构完整,业务活动相关的电子文件保留齐全时,电子文件的完整性(Completeness,齐全)能够为电子证据与待证事实之间的关联提供充足线索。

当电子文件满足可用性时,意味着业务活动的过程得以呈现,文件形成与利用的信息能够被检索,文件之间的联系可以被查找与定位,这有助于电子文件作为证据时与待证事实之间关联性的认定。

电子证据的合法性指证据调查主体、证据形式、证据的收集提取过程符合法律规定,不能由非核正程序或非法软件生成。其部分内涵对应了电子文件的安全性,即电子文件的来源系统合法、环境安全可靠、管理过程可控。

由上可知,电子证据的"三性"与电子文件的"四性"间的确存在关联,但这种关联是有限的。除电子文件的真实性、可靠性与完整性能够与电子证据的真实性实现完全映射外,电子证据的关联性与合法性仅能在电子文件"四性"中实现部分映射,无法实现映射部分属于司法取证与审判阶段,受到与案件事实的客观关系、取证与司法人员的实际操作等因素影响。

5 电子文件证据性概念模型的构建与适用

5.1 电子文件证据性概念模型的构建。除概念分析与映射阶段涉及的部分标准规范外,笔者还参考了ISO/IEC27001:2013(GB/T 22080-2016)、《信息技术 安全技术 信息安全管理体系 要求》、ISO 16175-1:2011《信息与文献 电子办公环境中文件管理原则与功能要求 第1部分:概述和原则》、GB/T 22240-2008

《信息安全技术信息系统安全等级保护定级指南》、DA/T 56-2014《档案信息系统运行维护规范》、DA/T-75-2019《档案数据硬磁盘离线存储管理规范》、建标103-2008《档案馆建设标准》、JGJ 25-2010《档案馆建筑设计规范》等国际国内标准对模型的构建过程进行论证，对各项概念的内涵进行解读。

如图2所示，电子文件证据性概念模型以“证据性”为核心，由内向外共可划分为三个圈层。

其中，第一、第二圈层的属性为内部属性，即用于描述电子文件本身品质的属性；第三圈层为外部属性，是用于描述电子文件管理环境与相关活动的属性。

三个圈层共计8个属性，共同阐释了位于中心的电子文件证据性。下文中如无特殊说明，真实性、可靠性等属性均指电子文件的属性而非电子证据的属性。

5.1.1 第一圈层：证据真实性相关属性。电子文件证据性概念模型的第一圈层包括真实性、可靠性与完好性三个属性，共同阐释了电子证据“三性”的核心——证据真实性。

真实性(Authenticity)：电子文件的内容、逻辑结构、形成背景三要素与形成时的原始情况相一致；电子文件的用意、生成者或发送者及其时间等关键条件与既定情况相符(主要参考来源：DA/T58-2014等)。

可靠性(Reliability)：电子文件的内容可信，能够充分、完全、准确、正确地证明其所反映的事物、活动或事实。电子文件还原客观事实的能力越强，则可靠性越高(主要参考来源：ISO15489；GB/T 26162.1-2010；GB18894-2016；DA/T58-2014等)。

完好性(Integrity)：指电子文件未被非授权改动、破坏、变异、丢失，即完好无损。此处完好性主要参考信息安全领域“Integrity”的定义。为了与电子文件“完整性”以及“齐全性”相区分，故表述为“完好性”(主要参考来源：GB/T 20984-2007；ISO/IEC 27001：2013；GB/T22080-2016等)。

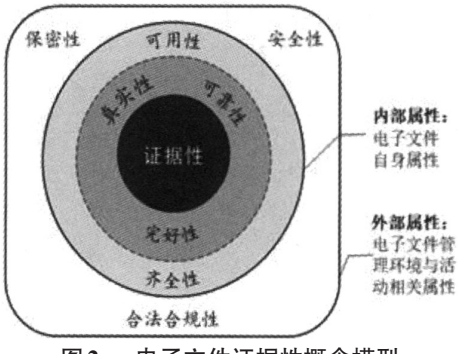

图2 电子文件证据性概念模型

5.1.2 第二圈层：证据关联性相关属性。电子文件证据性概念模型的第二圈层包括齐全性和可用性，这两个属性体现了电子文件与各项事务、业务活动的联系，有助于证据关联性的部分实现。

可用性(Usability)：指电子文件能够被定位、查找、检索、呈现、理解(主要参考来源：ISO15489等)。

齐全性(Completeness)：指电子文件本身的内容、背景与结构是齐全的，与业务活动和相关事务过程相关的电子文件被全面保存。(主要参考来源：ISO 15489；GB/T 26162.1-2010；GB 18894-2016；DA/T 58-2014等)。

5.1.3 第三圈层：证据合法性相关属性。电子文件证据性概念模型的第三圈层与前两个圈层性质不同，关注的不是电子文件本身所具有的属性，而是从安全性、保密性、合法合规性三个方面为电子文件的管理环境与管理活动提出要求，从而有助于为同样作为“外部”属性的证据合法性提供保障。

安全性(Security)：在档案学的语境中，安全性的概念十分广泛，它既可以是其他属性的实现基础，也可作为真实性、可靠性、完整性等其他属性应达到的最终目标。安全性以风险与故障的不发生为标准。

保密性(Confidentiality)[28]：在信息安全领域，对安全最基本的要求为“CIA”原则，即Confidentiality(保密性)，Integrity(完整性)，Availability(可用性)。[29]

本概念模型试引入其中“保密性”的概念，根据GB/T 20984-2007的规定，关键在于通过一系列技术手段实现权限的分配与执行。

在电子证据的取证中，对于取证操作过程“清洁性”的要求极为重要，与证据无关的程序、个人和组织不应接触到证据材料。

在本文所提出的电子文件证据性概念模型中，保密性具体表现在通过实施物理密保技术、访问控制技术、信息加密技术等防篡改技术措施使非授权的其他组织机构、业务部门、人员与其他程序与系统

与目标电子文件隔离[30]。本属性主要从技术视角对电子文件证据性加以阐释(主要参考来源:ISO/IEC 27001:2013;GB/T 22080-2016;GB/T 20984-2007等)。

合法合规性(Legitimacy and Compliance):即强调实现电子文件管理环境与管理活动的法规遵从。本属性主要从管理视角对电子文件证据性加以阐释(主要参考来源:ISO 16175-1:2011;GB/T 22240-2008等)。

5.2 电子文件证据性概念模型的适用。电子文件证据性概念模型运用档案学视角和适用于档案管理环境的术语重新阐释了司法对电子证据的要求,具有证据性的电子文件是电子证据的"前身",经过合法取证程序后能够在法庭上发挥其证据效力。

该模型将司法证明要求的真实性作为高应诉概率电子文件管理的核心目标并将合法性与关联性相关要求纳入电子文件管理目标。

综上,电子文件证据性概念模型在理论层面上初步实现了电子文件与电子证据的属性对接与要求转化。对于电子文件管理与电子证据司法应用业务层面的融合、司法对电子文件管理的具体要求、电子文件的凭证性保障策略等实践问题仍需文件与档案管理工作者与法律工作者协同合作、持续探索。

参考文献:

[1]冯惠玲,张辑哲.档案学概论[M].北京:中国人民大学出版社,2001:9.

[2]王健.网络狼烟——电子文件引发的管理悖论[J].山西档案,2002(03):8-12.

[3]DURANTI L, ROGERS C. Trust in Digital Records: An Increasingly Cloudy Legal Area[J]. Computer Law & Security Review, 2012, 28(05): 522-531.

[4]ROGERS C. Virtual Authenticity: Authenticity of Digital Records from Theory to Practice[D]. Vancouver: University of British Columbia, 2015: 183-185.

[5]张宁.电子文件的真实性管理[M].沈阳:辽宁人民出版社,2009:21-40.

[6]崔屏.电子文件凭证性溯源及内涵研究[J].档案与建设,2013(09):4-7.

[7][14]刘越男,李静雅.电子数据、电子文件相关概念的比较与对接[J].档案学研究,2017(S1):92-99.

[8]王燃.电子文件管理与证据法规则的契合研究[J].档案学通讯,2018(05):51-56.

[9]谢丽,范冠艳.电子文件与电子证据领域中的真实性概念分析[J].浙江档案,2019(01):13-17.

[10]为便于叙述,标准规范首次出现时均以全称表示,之后均以标准号代称.

[11]中国国家标准化管理委员会.GB/T 26162.1-2010信息与文献 文件管理 第1部分:通则[S].北京:中国标准出版社,2010.

[12]中国国家标准化管理委员会.GB/T 18894-2016电子文件归档与电子档案管理规范[S].北京:中国标准出版社,2016.

[13]DA/T 70-2018文书类电子档案检测一般要求[EB/OL].[2020-10-20].http://www.saac.gov.cn/daj/hybz/201806/51dc8c8f5864df49eaaeb82dfe8e193/files/c56f09e7648345baa692f82b4bdc4689.pdf.

[15]DA/T 58-2014电子档案管理基本术语[EB/OL].[2020-10-09].http://www.saac.gov.cn/daj/hybz/201806/11d12aaf89e4228a720b07fddffb480/files/4edded2147cc407fa4c72638eedc9726.pdf.

[16]孙大东.电子文件管理系统的认知[J].档案管理,2017(03):66-67.

[17]高爱民.建设项目施工阶段电子文件的真实性研究[J].档案管理,2019(01):42-43.

[18]冯惠玲,刘越男.电子文件管理教程[M].第2版.北京:中国人民大学出版社,2017:34.

[19]中国国家标准化管理委员会.GB/T 20984-2007信息安全技术-信息安全风险评估规范[EB/OL].[2020-10-30].http://www.doc88.com/p-1806006399273.html.

[20]国家档案局长李明华:强化红线意识加强档案安全工作[EB/OL].[2020-10-20].http://www.saac.gov.cn/news/2017-06/07/content_189108.htm.

[21]陈光中.证据法学[M].第3版.北京:法律出版社,2015:147-150.

[22]客观[EB/OL].[2019-10-18].https://www.zdic.net/hans/%E5%AE%A2%E8%A7%82.

[23]中国国家标准化管理委员会.GB/T 22080-2008信息技术 安全技术 信息安全管理体系[EB/OL].[2020-10-20].http://www.doc88.com/p-6941784346942.html.

[24][25]何家弘,刘品新.证据法学[M].第5版.北京:法律出版社,2013:114-115.

[26]何家弘,刘品新.电子证据法研究[M].北京:法律出版社,2002:122-124.

[27]孙锐.刑事证据资格研究[D].长春:吉林大学,2017:15.

[28]SAMONAS S, COSS D. The CIA Strikes Back: Redefending Confidentiality, Integrity and Availability in Security[J]. Journal of Information System Security, 2014, 10(03): 21-45.

[29]STAMP M.信息安全原理与实践[M].杜瑞颖,赵波,王张宜,等,译.北京:电子工业出版社,2007:1-2.

[30]朱璇.基于ISO 27001的信息安全管理体系的研究和实现[D].上海:上海交通大学,2009:5.