基于信息系统架构的信息资产分类与关系识别①

Classification and Relationship Identification of Information Assets Based on Information System Architecture

诸葛理绣　(衢州职业技术学院 现代教育技术中心 浙江 衢州 324000)

王军华　(浙江工业大学浙江分校 现代教育技术中心 浙江 衢州 324000)

周　晨　(中国工商银行衢州市分行 浙江 衢州 324000)

摘　要： 信息资产识别是信息安全风险评估工作的核心环节。文中提出了基于信息系统架构，涵盖信息安全相关的所有资产的一个参考分类框架，并在此基础上分析资产之间的依存关系。评估者以该框架为工具识别资产时，可以做到清晰、规范和全面。

关键词： 信息安全 风险评估 信息系统架构 资产分类 资产关系

1　引言

随着信息化的发展，政府部门、金融机构、企事业单位及各经济组织等对信息系统的依赖程度日益增强，信息安全问题受到普遍关注。作为信息系统建设过程中不可或缺的技术手段，信息安全风险评估就是从风险管理角度，系统地分析信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施，将风险控制在可接受的水平，从而最大限度地保障信息安全提供科学依据。

信息安全风险评估工作中，资产、威胁、脆弱性是三大主要风险因素[1]。其中资产作为衍生出脆弱性的母体、威胁的作用对象，使得信息资产识别成为信息风险评估工作的核心环节，因此资产识别的正确性和准确性对于后续的各风险要素及其综合评估至关重要。通过资产识别，明晰风险评估范围内与信息安全相关的资产清单、资产关系和资产价值，列出评估范围内关系到信息安全的所有资产，并按照资产的性质进行合理分类，梳理其之间关系，并就其价值进行赋值。

2　基于信息系统架构进行资产分类和资产关系识别

2.1 传统的信息资产分类方法

信息资产是具有价值的信息或资源，它能够以多种形式存在，有无形的、有形的，有硬件、软件，有文档、代码，也有服务、形象等[2]。通常，资产识别者要么利用自身掌握的概念和知识来识别相应信息系统范围内的信息资产，并自定义进行分类，如按数据、资产重要性等分类方法；要么采用 BS7799 及国家标准 GB/20984 基于资产表现形式的分类方法来识别评估范围内的信息资产。就前者而言，不同的资产识别者出于理解和能力的差别，对给定的对象范围会得出不同的资产分类及清单，如仅列出了技术方面的资产，而忽略了管理方面的资产，导致资产识别的偏颇或不完整[3]。此外，由于没有统一的分类标准，资产定义和分类因人而异，可能会导致评审人员交流和沟通上的困难。而就后者而言，在按照上述分类方法实施资产分析时，结合被评估对象具体特点，鉴于某些资产之间联系紧密，导致这些资产属性之间存在重叠部分进而对这些资产分别价值赋值，直接导致资产重复赋值，严重影响评估结果的准确度[4]。例如，对于

① 基金项目:浙江省衢州市科技计划(2007256)
收稿时间:2008-12-01

应用服务器，包括服务器硬件、操作平台及针对应用的相关服务，其实它们结合十分紧密，是以一个整体为业务提供服务的，无论是硬件故障，还是操作平台或服务因恶意代码影响都会造成信息系统运行中断或拒绝服务，使得业务数据的可用性受到影响，如果在可用性上分别为应用服务器硬件、软件和服务赋值，这就扩大了应用服务器在可用性的价值。所以，对于应用服务器，从安全需求和控制措施上，没有必要将它们分别考虑。

基于上述有关问题，下文提出一个基于信息系统架构且涵盖信息安全所有资产的标准分类框架。

2.2 信息系统的基本架构

从技术角度分析，构成信息系统的要素包括：

①业务数据，这里包括信息系统中存储、处理传输的电子数据，存储在备份介质中电子数据以及通过信息系统中输出的纸质数据等。

②应用平台，主要指的是基于业务逻辑和处理业务的应用系统。

③计算基础结构，主要包括网络、计算机、系统和支撑软件、数据交换协议以及其运行的基础环境等。

④其他数据载体，主要指备份数据的存储介质

⑤组织和制度，主要指系统管理员及业务用户、有关业务目标的操作规程以及信息系统的安全管理制度等。

依据各要素之间的逻辑支撑关系，其架构图如下：

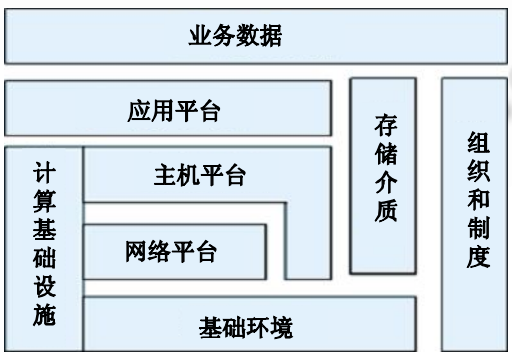

图 1　信息系统基本架构

2.3 信息资产分类

如图 1，1 级分类将资产分为业务数据、应用平台、存储介质、组织和制度、主机平台、网络平台、基础环境 7 大类别。如表 1 所示，业务数据包括电子业务数据、其他介质业务数据、操作规程等 3 个 2 级分类；计算基础设施是信息系统的技术基础设施，具体包括主机平台、网络平台、基础环境等 3 个 1 级分类，其中主机平台又包括客户机、应用服务器、数据服务器、外部设备等 4 个 2 级分类，网络平台包括 PDS、交换机、路由器、网络安全设备等 4 个 2 级分类，基础环境包括计算场所、电力保障(设备供电及照明)、空调、通讯设施、消防设施等 5 个 2 级分类；应用平台是运营业务数据的信息系统应用软件，包括应用软件、程序代码及相关技术文档等 3 个 2 级分类；存储介质指的是业务数据在应用平台外的保存方式，包括业务数据的备份介质及纸制记录等 2 个 2 级分类；组织与制度指的是系统的组织和制度方面的保障，包括系统管理员、普通用户、业务合作方、管理制度等 2 级分类。

表 1　基于信息系统架构的资产分类框架

1 级编号	1 级分类名	2 级编号	2 级分类名称	3 级编号	3 级分类名称
1	称业务数据	1.1	电子业务数据		
		1.2	其他介质业务数据		
		1.3	操作规程		
2	应用平台	2.1	应用软件		
		2.2	程序代码		
		2.3	技术文档		
3	存储介质	3.1	备份介质		
		3.2	纸制记录		
4	组织与制度	4.1	系统管理员		
		4.2	普通用户		
		4.3	业务合作方		
		4.4	管理制度		
5	主机平台	5.1	客户机	5.1.1	硬件
				5.1.2	操作系统
				5.1.3	技术文档
		5.2	应用服务器		
		5.3	数据服务器		
		5.4	外部设备		
6	网络平台	6.1	PDS		
		6.2	交换机		
		6.3	路由器		
		6.4	网络安全设备		
7	基础环境	7.1	计算场所		
		7.2	电力保障		
		7.3	空调		
		7.4	通讯设施		
		7.5	消防设施		
		7.6	安防设备		

在评估过程中，基于信息系统架构的资产分类，关键是将受评单位的各种业务识别出来，并进行边界确认，然后进行比较和决策，确定业务优先级，然后根据该分类方法区分资产[5]。在评估实务中，资产分类框架的内容和级别数目可根据行业或机构的不同有所区别。一般而言，高层的分类内容基本是一致的，越往底层其分类内容越反映行业或机构的特点。另外，所评资产的分类级别数目有时不易过细。比如说，表 1 中的客户机在分类级别 3 中可以进一步分为计算机硬件、操作系统及相关技术文档三类。在实务中，它们特别是硬件和操作系统是以整体向上面应用平台和用户提供支撑和服务的，如果分别考虑，会造成资产属性之间存在重叠(如可用性)，接下来对这些资产分别资产赋值，会导致资产重复赋值，严重影响评估结果的准确度。基于信息系统架构的资产分类框架非常便于各受评单位自评层面上的资产识别与管理，表 1 提出的信息资产分类框架可在评估实践中产生、确定和规范化。

2.4 信息资产关系分析

事实上，信息资产是有机结合和协同工作的，是以整体方式来实现受评单位业务目标的。因此，信息资产之间必然存在着依存关系。这种“依存”关系有三层含义：(1)被依赖方“承载”依赖方，如计算基础设施各类资产承载上层的应用平台资产，应用平台及存储介质类资产承载上层的业务数据资产，而在计算基础设施中，基础环境类资产承载上面的网络平台类资产等；(2)被依赖方对业务目标的贡献通过上面的依赖方来实现的；(3)依赖方资产的安全属性价值通过这条链传递给被依赖方。为此，我们可以从业务目标出发，根据信息系统架构，依托信息资产之间的依存关系，形成业务目标为根节点的资产关系图。图 2 给出了结合信息系统架构的资产基本依存关系图。当然，在评估实务中，可以以更高的资产分类级别和具体的资产进行细划。

3 结束语

信息资产的识别、分类及安全价值评估是信息安全风险评估工作的重要环节。文中提出的基于信息系统技术架构的信息资产分类识别方法，逻辑性强，层次清楚，便于进行资产分类和关系分析，梳理出关键资产，可为更进一步资产价值评价及后续的风险评估和风险管理工作奠定良好基础。

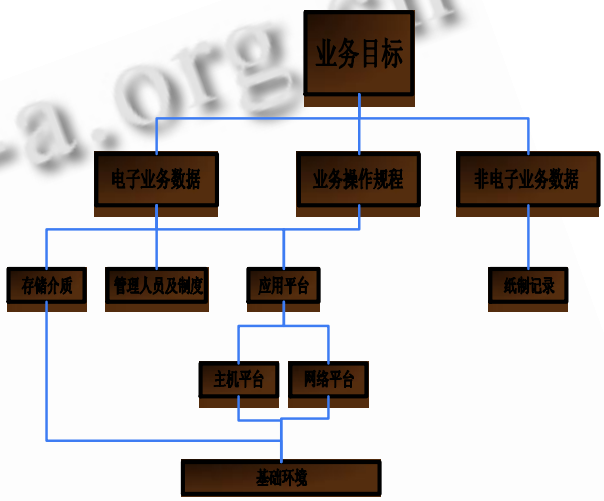

图 2　信息资产关系示例图

参考文献

1 GB/20984, 信息安全风险评估规范.
2 范红,冯登国,吴亚非.信息安全风险评估方法与应用.北京:清华大学出版社,2006:34－38.
3 陈伟.信息资产分类与控制.中国计算机用户, 2004, 18:56.
4 傅鹂,刘嘉伟,周贤林.基于业务的信息资产识别方法.通信技术,2007,40(12):238－240.
5 闵京华.信息安全的资产评估方法.信息网络安全, 2006,1:28－30.