doi:10.3969/j.issn.1000-436x.2014.z1.034

数字校园中管理信息系统安全体系结构设计与应用研究

龙新征，邢承杰，欧阳荣彬，王倩宜，李丽，刘云峰
(北京大学 计算中心，北京 100871)

摘 要：针对高校管理信息系统面临的安全威胁和挑战，提出了 1C4GS 安全体系结构，阐述了 1C4GS 的 5 个重要组成部分：安全管理中心、安全通信网络、安全区域边界、安全计算环境及安全应用系统的内涵和作用。以数字校园典型案例——“个人基本事项申报系统”为例，构建了基于 1C4GS 的高校管理信息系统安全应用方案，对包括透明数据加密，用户身份鉴别，表单编辑缓存在内的多种安全技术和策略进行了有机整合，实现了管理信息系统的网络安全、边界安全、计算环境安全和应用系统安全。
关键词：管理信息系统；安全体系结构；透明数据加密；用户身份鉴别；表单编辑缓存
中图分类号：TP315 **文献标识码**：A **文章编号**：1000-436X(2014)Z1-0178-07

Design and application research on management information system security architecture in digital campus

LONG Xin-zheng, XING Cheng-jie, OUYANG Rong-bin, WANG Qian-yi, LI Li, LIU Yun-feng
(Computer Center, Peking University, Beijing 100871,China)

Abstract: Aiming at the university management information system security threats and challenges, a security architecture named 1C4GS was proposed. First connotation and function of five important components of 1C4GS was expounded, which named security management center, security communication network, security region boundary, security computing environment and security application. Then we used “basic personal data reporting system” as an example to construct the management information system security arrangement application based on 1C4AS, this arrangement application integrated a variety of security technologies and strategies such as transparent data encryption, user Identify, form edit cache as a whole ~~to~~, and achieved the management information system’s network security, border security, computing environment security and application security.
Key words: management information system; security architecture; transparent data encryption; user identify; form edit cache

1 引言

随着数字校园建设的不断深入，高校的教学科研及管理服务等日常工作对管理信息系统（MIS, management information system）的依赖度越来越高。MIS 在给各院校工作带来便利的同时，也面临着安全威胁和挑战，集中表现在以下几个方面：1）面临双重威胁：不但容易受到来自 Internet 的攻击，而且面临校园网内部的安全威胁；2）用户身份复杂，应用需求各异：不同需求对身份认证和访问控制提出了更高要求；3）数据量大，数据敏感度不同，安全级别各异：在实施安全保护时必须针对各自的敏感度及服务对象采取不同级别的安全策略，即使是对某一项信息，如学生基本信息，它们的有些数据必须实行更高级别的保护，安全粒度更细。

高校 MIS 安全问题受到越来越多的重视。本文在以往研究基础上，设计了 1C4GS 安全体系结构，并实现了基于 1C4GS 的 MIS 安全应用方案。本文

收稿日期：2014-10-18
基金项目：国家发改委 2011 信息安全专项基金资助项目
Foundation Item: Project of NDFC 2011 Information Security

具体工作包括以下内容。

1) 设计了 1C4GS 安全体系结构，由安全管理中心、安全应用系统、安全计算环境保障、安全区域边界、安全通信网络 5 部分组成。

2) 实现了基于 1C4GS 的 MIS 安全应用方案，将包括透明数据加密、用户身份鉴别、表单编辑缓存在内的多种安全技术和策略进行有机整合，形成完整统一的安全体系，对 MIS 的网络安全、边界安全、计算环境安全、应用安全起到了有效的保护。

2　相关研究分析

高校 MIS 安全领域主要包括身份认证、访问控制、授权、数据加密保护、数据完整性保护、数据不可否认性保护、审计和日志管理等，针对这些领域出现了越来越多成熟的技术和策略，如：基于数字认证的身份认证技术、基于角色的访问控制技术、基于 PKI/CA 的加密和数字签名技术等。对安全技术和策略的研究是 MIS 安全的重要课题，也是本文的研究内容。

尽管安全技术和策略很多，但在实际应用中，如果安全技术和策略不能形成完整统一的安全体系，就会造成开发成本的提高和安全技术复用性的降低。

Intel 的体系结构实验室于 1996 年提出了公共数据安全体系结构(CDSA, common data security architecture)[1]，这是一个基于模块和层次的安全体系结构，定义了 3 个层次，逐级向上提供服务：最底层是实现基本算法的插件式安全模块，包括加密算法和证书处理等组件；这些基本功能模块在核心部分公共安全服务管理器(CSSM, common security services manager)的协调下向最顶端的系统安全服务层(SSS, system security services)提供服务。这种基于模块的方式与应用系统耦合度较大，不适宜高校 MIS 的实际情况。

胡志昂等人提出了“一个中心”管理的“三重保障”安全应用平台[2]。一个中心是指安全管理中心；三重保障是指安全计算环境、安全区域边界和安全通信网络，平台比较符合高校 MIS 的实际部署情况，但也存在需要完善的地方。一是没有考虑应用系统自身的安全性；二是在安全策略的制定和选取方面阐述较少。基于此，本文进行修正，提出了 1C4GS 安全体系结构，将安全应用系统纳入安全体系结构的范畴，并制定了符合数字化校园实际情况的安全策略。

3　1C4GS 安全体系结构

1C4GS 安全体系结构如图 1 所示。1C 是一个中心，即安全管理中心；4GS 表示四重保障：安全通信网络、安全区域边界、安全计算环境以及安全应用系统。

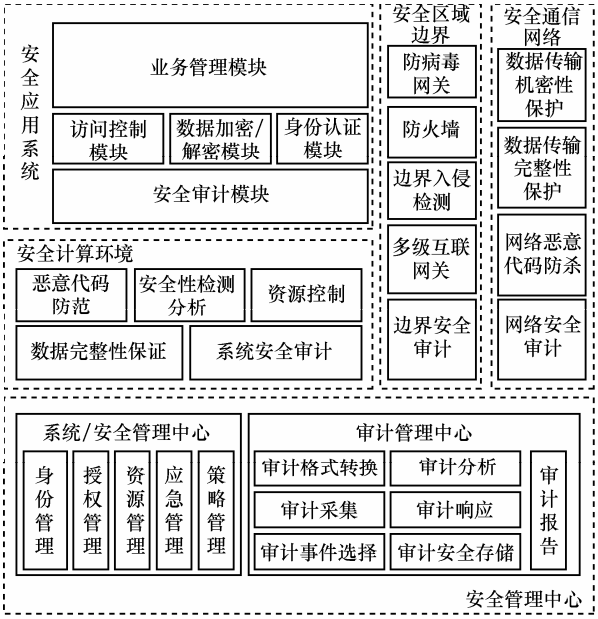


图 1　安全体系结构 1C4GS

1) 安全通信网络（security communication network）。通过网络管理系统对网络线路状况、网络设备的性能与运行状况进行监控和管理；通过恶意代码防范系统实时查杀病毒、定期扫描病毒，并提供及时升级病毒；通过网络安全审计采集和记录所有用户通过网络访问资源的行为日志，并进行管理分析、告警、统计、查询；通过网络数据传输加密机制确保数据在内外网之间传输和交互时的保密性；通过网络数据传输完整性检测确保数据在内外网之间传输和交互时的完整性。

2) 安全区域边界(security region boundary)。通过防火墙和防病毒网关提供逻辑隔离、应用代理、访问控制和信息过滤，并记录边界违规行为；通过边界入侵检测系统检测边界入侵，拒绝服务攻击的行为并产生日志记录；通过多级互联安全网关提供不同安全级别之间的网络和信息系统之间的可控访问和数据交换。

3) 安全计算环境(security computing environment)。包括操作系统安全和数据库安全。通过恶意代码防范系统实时查杀病毒、定期扫描病毒，并提

供及时升级病毒；通过终端和主机行为审计系统采集主机服务器操作系统和数据库管理系统自身的日志信息；通过系统安全性检测分析及时发现操作系统及数据库管理系统的漏洞和脆弱性；通过制定服务器操作系统的用户策略、密码策略、访问控制策略、审计策略以及资源控制策略保障服务器操作系统的安全；通过制定数据库管理系统加密和屏蔽策略、访问控制策略、审计和监制策略以及阻止和记录策略保障数据库的安全。

4) 安全应用系统(security application)。通过特定的模块提升应用系统的安全性，这些特定的模块包括身份鉴别模块、访问控制模块、数据加密/解密模块、应用审计模块等；同时加强对代码自身漏洞的检测和预防，严防 SQL 注入、跨站脚本攻击等严重错误；通过代码扫描工具对源代码进行扫描。

5) 安全管理中心(security management center)。对安全网络、安全边界、安全计算环境以及安全应用系统进行监控和管理，包括系统/安全管理中心和审计管理中心；系统/安全管理中心对安全网络、安全边界、安全计算环境的用户、权限、应急措施、策略进行统一的管理；审计管理中心对安全网络、安全边界、安全计算环境的日志进行统一的管理分析、告警、统计、查询。

4 1C4GS 应用研究

1C4GS 给数字校园带来了安全的环境、安全的应用系统和安全的管理中心。下面以数字校园典型案例——“个人基本事项申报系统”（以下简称申报系统）说明基于 1C4GS 的安全应用平台的建设和具体安全机制的实施。

4.1 系统简介

申报系统是一个 B/S 系统。用于学校教职员工填写并申报个人的基本情况，有关管理部门的管理人员查看并审核教职员工申报的信息，并对信息进行统计。业务流程如图 2 所示。

申报系统中有 4 类用户角色。

1) 申报用户：主要功能是对自己的个人填报信息查看、修改、保存和提交。

2) 管理部门工作人员：主要功能是查看、审批和统计申报用户提交的填报信息。

3) 系统管理员：主要功能是维护申报用户名单，授权管理部门工作人员维护。

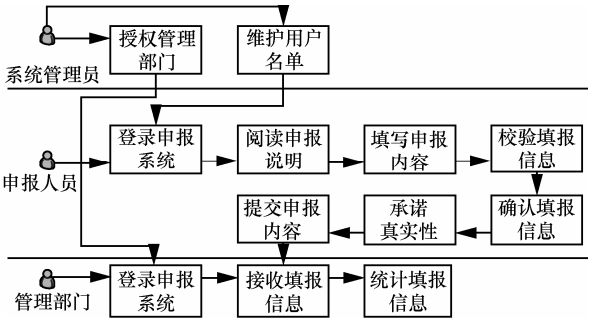


图 2 “个人基本事项申报系统”业务流程

4) 审计管理员：对申报用户、管理部门工作人员、系统管理员的操作进行审计。

申报人员是全校教职员工中的部分人员，他们有可能在办公室申报，也有可能在家里甚至在出差途中或者国外访问期间申报，因此申报系统只面向校园网是不现实的，而是应该基于校园网环境，架构在互联网之上，全球可访问；申报人员填写的个人信息涉及个人隐私，安全级别非常高，除了申报人员本人和管理部门工作人员之外，任何人都不能获得这些信息。3 类管理人员人数少但权限非常高，一旦安全措施出现漏洞，将导致全系统的信息泄露。

4.2 安全区域边界和安全通信网络

1C4GS 架构下，申报系统的网络结构如图 3 所示。

为保证通信网络安全，在校园网边界配备了 10 Gbit 校园网防火墙(华为 USG95)，在电子校务机房配备了吉比特防火墙(山石 SG-6000)，并在校园网边界配置了 VPN 设备(Juniper SA-4500)提供 SSL VPN 访问。

为保证区域边界安全，在校园网内部划分了 3 个专网。申报系统用户任意地址登录 SSL VPN 后获得专用网段 VLAN3（不同于其他普通用户，只能校外登录 SSL VPN 后获得通用网段 VLANx）；申报系统应用服务器专用网段 VLAN2；申报系统数据库服务器专用网段 VLAN1。并制定了严格的网络访问控制策略：只允许 VLAN2 访问 VLAN1；只允许 VLAN3 访问 VLAN2；只允许通用网段 VLANx 访问教育网免费地址。通过专用网段的划分以及网络访问控制策略的设置，将申报系统与校园网的其他部分完全隔离开来。

4.3 安全计算环境

申报系统计算环境包括 4 台专用服务器：Web 应用系统服务器主机、Web 应用系统服务器备用机、数据库系统服务器主机和数据库系统服务器备用机。通过设置服务器冗余的方式，保证系统的高可用性，当主机宕机时，可以启用备用机。在数据库

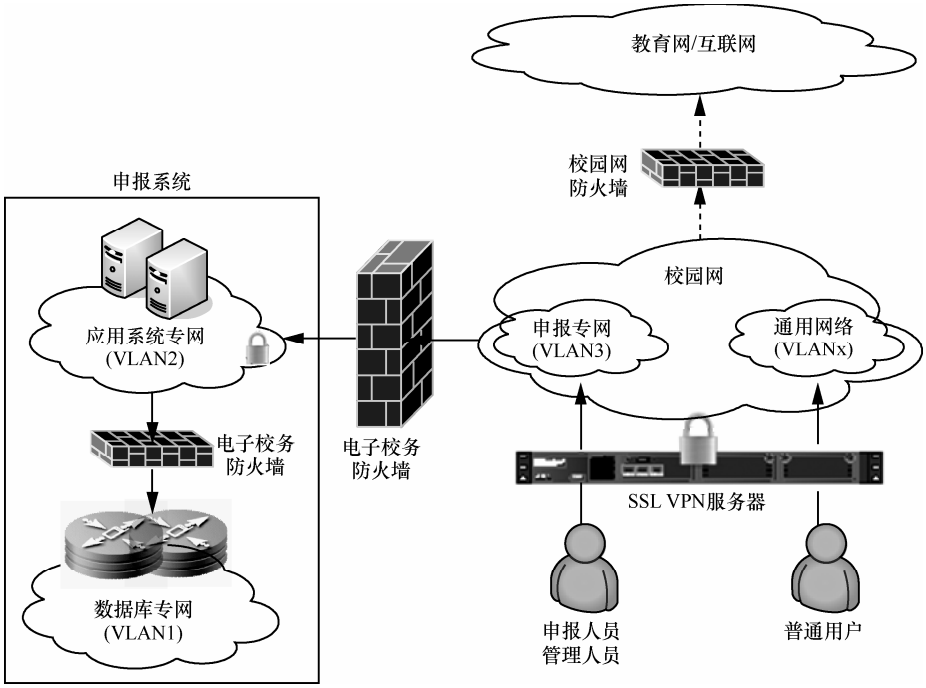


图 3　“个人基本事项申报系统”网络结构

表 1　　**服务器操作系统安全具体措施**

策略	措施
用户策略	用户账号尽可能少，且尽可能少地用来登录
密码策略	所有用户账号都设置复杂的口令，长度最少在 12 位以上，且必须同时包含字母、数字、特殊字符； 设置强制密码历史为 5 次，时间为 30 天
访问控制策略	开启防火墙； 仅开启必需的服务端口，将其他不必要的端口全部禁用； 禁止远程终端方式访问服务器； 只允许经专用网段 VLAN3 的特定 VPN 地址访问 Web 应用服务器的 Web 端口； 客户端必须以加密形式访问服务器； 数据库服务器只开放一个端口给 Web 应用服务器访问
资源控制策略	操作系统遵循最小安装原则，仅安装需要的组件和应用程序
审计策略	启用操作系统和数据库自带的日志记录

系统服务器和数据库系统服务器备用机都安装了 Oracle 数据库。

4.3.1　操作系统安全

1C4GS 架构下，操作系统安全具体措施主要包括用户策略、密码策略、访问控制策略、审计策略以及资源控制策略等（如表 1 所示）。

4.3.2　数据库安全

数据库安全的目标是敏感数据“看不见”，核心数据“拿不走”，运维操作“能审计”。限于篇幅关系，简单介绍访问控制技术以及数据加密技术。

1) 访问控制

访问控制防止非授权用户非法访问数据库资源。在申报系统数据库中，数据资源包括以下 3 类：填报信息有关的数据库表(RT)、用户信息数据库表(UT)和审计信息数据表(AT)。用户角色与申报系统的 4 类用户角色一一对应：申报用户(RU)、管理门工作人员(MU)、系统管理员(SU)、审计管理员(AU)。数据库访问控制策略如表 2 所示。

2) 加密技术

数据库加密技术对数据库中的敏感信息进行加密，以密文的形式保存于物理数据库中。传统加密机制有库外加密和库内加密 2 种，库外加密需要编写复杂的加/解密程序，给应用程序带来了很大负担，并且频繁的加密解密影响用户的操作体验；库内加密密钥的管理复杂，完全基于访问控制，对数据库的性能影响比较大[3]。

Oracle 公司在 Oracle 10g Release 2 中提出透明数据加密(TDE, transparent data encryption)[4]，

表 2 数据库访问控制策略

用户角色	RT				UT				AT			
	查询	增加	删除	修改	查询	增加	删除	修改	查询	增加	删除	修改
RU		√						√		√		
MU	√		√		√			√		√		
SU					√	√	√	√		√		
AU									√			

TDE 兼具库外加密和库内加密二者的特点，它实现了密钥与加密数据的分开保存，从而提高了安全性，它又是一种库内加密，操作简单，过程对用户完全透明。

在 TDE 过程中，只要设置表中需要加密的表列，数据库会为该表自动产生“表密钥”对数据进行加密，TDE 方法会应用“主密钥”的密钥再对这些“表密钥”进行加密。用主密钥加密后的“表密钥”统一存储在数据库的数据字典中，而“主密钥”存储在服务器的 wallet 文件中，需要用户提供口令才能登录。这样就实现了密钥与加密数据的分开存储。

存储数据时，如果该表没有“表密钥”，系统首先生成一个“表密钥”，对数据进行加密，“表密钥”作为数据被“主密钥”加密后存储在数据字典中；如果该表已有“表密钥”，系统先从 wallet 中读出“主密钥”，在数据字典中读出“表密钥”并解密，接着使用解密后的“表密钥”对表中需要加密的数据进行加密，最后将密文数据存储在物理数据库中，整个执行过程对申报系统用户而言是透明的。

读取数据时，依然按照上述过程，先读取“主密钥”，对“表密钥”进行解密，然后使用解密后的“表密钥”对表中的密文进行解密，将明文返回。

使用这种加密方式产生的加密数据就算被窃甚至磁盘丢失，没有主密钥是无法解密数据的；即使 wallet 文件也被窃取，在没有登录口令的条件下，数据也一样不会泄露的。从而提高了数据的安全性。

4.4 安全应用系统

1C4GS 架构下，申报系统在身份鉴别、表单缓存、应用审计、软件容错方面采取措施。

4.4.1 用户身份鉴别

采用专用的登录控制模块对用户进行身份标识和鉴别。通过登录控制模块，系统管理员可以添加其他 3 类用户，与之关联的是给他们数据授权和功能授权。授权成功后，用户具有访问相应数据和功能的权限。

无论何种用户，登录系统时都要经过 2 次身份验证。

第一次是通过校园网用户名和密码登录 SSL VPN，进入申报系统专用网段 VLAN3，VLAN3 只对特定的用户开放，即需要申报材料的教职员工、管理部门工作人员、系统管理员以及审计管理员，所有无权限用户将会被挡在 VLAN3 之外。

第二次是成功进入 VLAN3 后从登录界面登录申报系统，考虑到 4 类用户角色的不同特性，对申报用户和 3 类管理人员采用了不同的身份认证策略。

对于 3 类管理人员，他们人数少，权限大，安全级别高，采取基于数字证书的 USBKEY 身份认证方案，需要给他们都配备专门的 USBKEY。

对于申报用户，他们人数众多，使用 USBKEY 成本太高，且申报用户可能不在学校，短时间内发放 USBKEY 不切实际，因此采用用户名+密码+动态验证码加强填报人的身份鉴别：密码是系统管理员添加申报用户时系统自动随机生成的，生成的同时通过短信明文通知申报用户，密码将加密存储在数据库中，系统管理员不能查看，但可以重置密码；每次登录时，申报用户输入正确的用户名和密码后，会通过手机动态获取 6 位验证码，验证码 1 min 内有效，申报用户正确输入动态获取的验证码即可登录系统，登录系统之后，本次动态验证码自动失效。动态验证码登录方式具有动态性、随机性、一次性、时效性和抗穷举性的特点[5]，加强了申报用户登录系统时的身份鉴别。

4.4.2 表单编辑缓存

表单编辑缓存是为了减少申报用户 SQL 操作申报系统数据库的次数：SQL 操作申报系统数据库的次数越多，数据库的安全隐患就越大。

具体做法是：申报用户填写编辑过程中的表单信息以加密 XML 文件的方式自主缓存在本地机器上，继续填报时，申报用户可以在申报系统中打开本地缓存文件；申报用户只有在提交表单操作时，会一次性将填报内容插入到数据库中，申报用户提

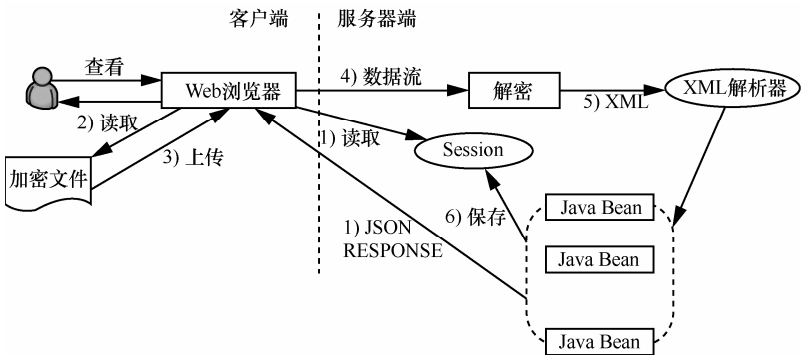


图 4　申报用户读取填报内容逻辑流程

交后将不能修改表单；申报用户不能从数据库中读取填报信息有关的那些数据库表，只能从本地缓存文件或者 Session 中读取自己填写填报信息。因此，在申报系统中连接数据库的申报用户只有“填报状态”的查询权限以及各填报内容表的插入权限。从而最大限度地保护了数据库系统的安全性。

图 4~图 6 分别说明了申报用户读取、保存和提交填报内容时的逻辑流程。

如图 4 所示，申报用户读取填报内容并不是从数据库中读取的，而是首先从服务器端的 Session 中读取。如果从 Session 里读取不到，则在本地缓存文件中读取；本地缓存文件是一个加密的 XML 文件，Web 浏览器将其读取后，以数据流的方式传到服务器端，服务器端按照约定的解密算法将其解密，解密的结果是符合规范的 XML 格式的字符串，通过 XML 解析器转换成与申报内容相对应的 java bean，保存到 session 中，同时以 json response 的形式返回给客户端，供申报用户查看。

如图 5 所示，申报用户保存填报内容并不是将数据保存到数据库中，而是首先保存到本地缓存文件，同时保存到服务器端的 Session。当点击保存按钮时，通过 Web 浏览器将需要保存的数据以 json 串的形式发送给服务器端，服务器端将他们直接保存到 Session 中，同时对其进行加密处理，以文件流的形式传给客户端，客户端通过 Web 浏览器接收到文件流后对其进行保存，可以选择新存一个文件，也可以选择对原有文件进行覆盖。

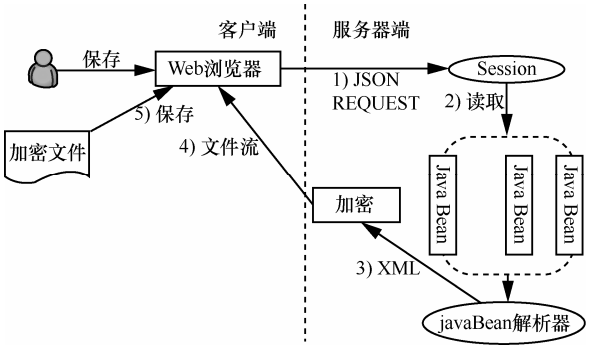


图 5　申报用户保存填报内容逻辑流程

如图 6 所示，只有当申报用户提交填报内容时才会将数据保存到数据库中，同时也保存到本地缓存文件和服务器端的 Session。这个过程与图 4 所示过程基本一致，所不同的是多了往数据库表中插入填报表单的数据，需要指出的是：这个插入过程要对多个表进行插入处理，因此一定要做事务操作。

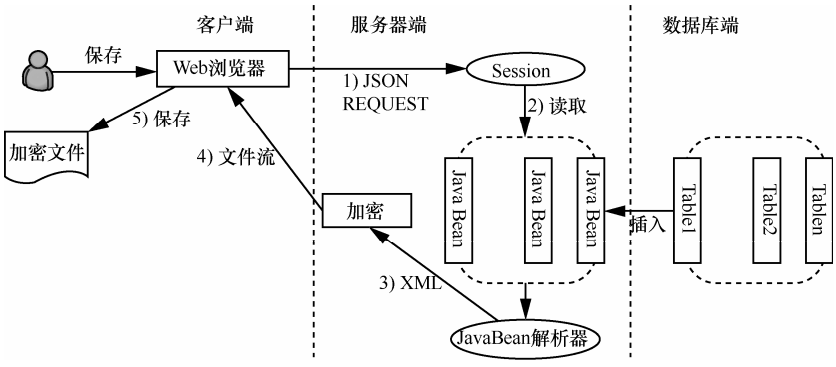


图 6　申报用户提交填报内容逻辑流程

4.4.3 应用审计

申报系统提供专门的应用审计模块，包含日志采集和日志浏览等功能。日志采集对申报用户、管理部门工作人员、系统管理员登录系统以后的操作行为进行日志记录，存储在数据库专门的审计信息数据表(AT)中。为了提高系统的安全度，除了实实在在对数据库中数据产生影响的新增、修改、删除等操作需要记录日志外，其他通过应用系统执行的任何操作，例如查询、导出等，也都需要记录日志；特别是对于修改操作，日志粒度应该尽可能细一些，例如：管理部门工作人员修改了申报用户信息，应该细化到修改了哪些字段的内容；原值是什么；新值是什么等，此外操作用户、操作用户、操作类型、操作说明、操作来源的模块、前台页面、操作时间等都需要进行记录。日志浏览提供给申报系统的审计管理员查询日志的功能。

4.4.4 软件容错

为防止利用源代码的漏洞攻击系统，加强了申报系统的软件容错能力。对于在 B/S 架构下常见的代码漏洞 SQL 注入、跨站脚本攻击等采用了必要的方法措施，例如：采用白名单，检测字符串变量的内容，只接受所需的值；检测用户输入内容的大小和数据类型，强制执行适当的限制与转换；此外，还采用了专门的代码扫描工具，对源代码进行扫描，及时发现并更正源代码的漏洞，最大限度地降低源代码漏洞带来的风险。

4.5 安全审计

安全审计包括通信网络安全审计，区域边界安全审计，安全计算环境安全审计和应用系统安全审计，其中应用系统安全审计由应用审计模块提供，其他由审计管理中心统一实施安全审计。审计管理中心可以采用搭建第三方审计系实现。鉴于篇幅问题，本文不作赘述。

5 结束语

本文以现有应用安全技术为基础，结合高校 MIS 的安全特性，提出了“一个中心”管理下的“四重保障”的 MIS 安全体系结构 1C4GS，对其重要组成部分——安全边界、安全网络、安全计算环境及安全应用的涵义进行了阐述；并结合数字校园中的一个典型案例“个人基本事项申报系统”，列举了安全体系结构的具体安全机制。该安全体系结构能有效地满足数字校园的安全特性，对于促进高校的信息安全建设具有一定实用价值。

参考文献：

[1] 郜宪林. DGSA、SSAF 和 CDSA 安全体系结构比较与分析[J].计算机工程与应用,2002,(3):96-98,113.
GAO X L. Comparison and analysis of DGSA,SSAF and CDSA[J]. Computer Engineering and Applications,2002,(3):96-98,113.

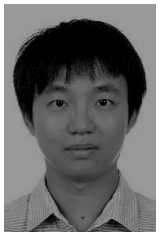
[2] 胡志昂, 范红.信息系统等级保护安全建设技术方案设计实现与应用[M].北京:电子工业出版社, 2010.
HU Z A, FAN H. Implementation and application of the Technology Scheme Design of Information System Security Protection Grade Construction[M].Beijing: Publishing House of Electronics Industry,2010.

[3] 黄志球.数据库应用技术基础[M].北京:机械工业出版社,2003.
HUANG Z Q. Database Application Technology Basic[M]. Beijing: China Machine Press,2003.

[4] 程敏，宋金玉. Oracle 数据库透明数据加密方式研究[J]. 信息安全与通信保密,2007,(8):153-155.
CHENG M, SONG J Y. Research on transparent data encryption of Oracle database [J].Information Security and Communications Privacy, 2007,(8):153-155.

[5] 卢加元,包勇.远程访问服务中的身份认证技术[J].计算机工程与设计,2005,26(7):1762-1764.
LU J Y, BAO Y. Identity authentication technology in remote access service[J]. Computer Engineering and Design, 2005,26(7):1762-1764.

作者简介：



龙新征（1984-），男，湖南湘阴人，北京大学工程师，主要研究方向为数据库应用技术、高校教育信息化等。

邢承杰（1978-），男，北京人，北京大学工程师，主要研究方向为数据库应用技术、高校教育信息化等。

欧阳荣彬（1979-），男，湖南宜章人，北京大学高级工程师，主要研究方向为数据库应用技术、高校教育信息化等。

王倩宜（1972-），女，辽宁大连人，北京大学高级工程师，主要研究方向为数据库应用技术、高校教育信息化等。

李丽（1980-），女，湖北黄州人，北京大学高级工程师，主要研究方向为数据库应用技术、高校教育信息化等。

刘云峰（1973-），女，山东莘县人，北京大学高级工程师，主要研究方向为数据库应用技术、高校教育信息化等。