

一种国际业务信息安全防护模型

蒋诚智¹, 刘婷婷², 余 勇¹

(1. 中国电力科学研究院 国家电网公司信息网络安全实验室, 江苏 南京 211106;
2. 南京工程学院 通信工程学院, 江苏 南京 211167)

摘 要:企业国际化经营是进一步拓展发展空间与提升可持续发展能力的有效途径,国际业务及其信息化建设的发展同时也给企业信息安全提出了新的挑战。文中针对电网企业国际业务及其信息安全的特点,提出了一种国际业务信息安全防护模型。在分析电网企业国际业务安全风险的基础上,从安全防护模型的主站层、网络层和终端层三个层次研究了安全防护技术措施,并提出了安全管理思路及措施。

关键词:国际业务;安全技术;安全管理

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2014)01-0158-05

doi:10.3969/j.issn.1673-629X.2014.01.041

An Information Security Protection Model for International Business

JIANG Cheng-zhi¹, LIU Ting-ting², YU Yong¹

(1. State Grid Information Network Security Laboratory, China Electric Power Research Institute,
Nanjing 211106, China;

2. School of Communication Engineering, Nanjing Institute of Technology, Nanjing 211167, China)

Abstract: International business is an effective way for enterprises to extend their business areas and to enhance their sustainable development capability, while the development of international business and its informationization brings challenge to information security of enterprises. In this paper, according to features of international business and information security in electric power grid companies, an information security model for international business is proposed. Based on security risk analysis, the security technical measures are studied from station level, network level and terminal level of the proposed model. Besides, the security management ideas and measures are also provided.

Key words: international business; security technology; security management

0 引 言

“加快实施‘走出去’战略”已被写入国家“十二五”规划中。央企实施国际化战略,不仅可以有效拓展业务发展空间,提升企业的可持续发展能力,还能有效带动上下游整个产业链的发展和国际竞争力提升,将有利于深化国家与新兴市场国家的战略合作关系,扩大国家在世界政治、经济格局调整过程中的战略影响,提升国家软实力。国家电网公司“十二五”国际发展规划中,拟推进海外电力投资运营、国际电力能源合作、电工电气设备制造、国际电力工程、国际电力技术和管理咨询、国际交流与合作等业务。国家电网公司

目前已经成功投资菲律宾、巴西和葡萄牙等国家的输电企业,同时在美国、俄罗斯、欧洲、巴西、菲律宾、印度、香港、委内瑞拉、葡萄牙、南非等多个国家和地区筹备或设立海外办事处。各直属单位和省公司也在装备、工程、贸易等方面开展了国际业务。同时,在国际业务及其信息化的发展过程中,面临着物理安全风险(例如,驻外机构信息系统的物理环境安全风险)、终端安全风险(例如,驻外机构办公计算机数据泄漏风险)、网络传输安全风险(例如,重要业务数据传输时被窃取与篡改的风险)及应用与数据交互安全风险(例如,非授权用户访问业务系统的风险)等。因此,需针对具体安全风险,同步进行安全防护设计,从各个

收稿日期:2013-03-27

修回日期:2013-07-03

网络出版时间:2013-11-12

基金项目:国家电网公司管理咨询项目(SGXXRKT[2012]856)

作者简介:蒋诚智(1982-),男,江苏南京人,博士,工程师,CCF会员,研究方向为信息安全、安全管理;余 勇,博士,研究员级高级工程师,研究方向为安全测评、安全管理。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20131112.1634.010.html>

层面建立信息安全保障措施,防止发生重要业务数据、敏感信息等泄漏的安全事件。

1 国际业务信息化策略

国际业务信息安全防护需紧密结合国际业务信息化方案与建设进程,根据业务应用类型及部署方式等进行相应的设计。根据业务板块规划,国家电网公司国际业务规划分为专业类业务应用与通用类业务应用。专业类业务应用主要包括电网运行管理等电网类业务应用、电源生产管理等电源类业务应用、电力工程管理等工程类业务应用、生产制造管理等电力设备类业务应用。通用类业务主要包括项目管理、人力资源管理、财务管理、物资管理等。

国际业务应用部署策略需从管控模式、业务模式、网络环境、法律法规要求、成本等方面综合考虑。根据信息化统一建设的原则,国际业务应用原则上尽量考虑集中部署。在管控模式方面,对国际业务有战略层、经营层和操作层上的管控要求,可考虑集中部署企业级决策、规划类应用、辅助决策类应用及生产管理类应用等;在业务模式方面,对于全资或控股的海外机构,可以主导进行信息化建设,在考虑业务应用特点的基础上决定部署策略。对于参股类海外机构,可考虑建立双方达成共识的数据上报标准,并提供数据上报途径。对于海外办事处、联络处及临时项目组等小型机构类型,可主要考虑建立远程访问国内相关系统的途径;在网络环境方面,对于网络环境较好的海外机构,可考虑在国内集中部署相关应用,海外单位通过远程接入访问。对于网络环境较差或暂不具备网络环境的海外机构,可考虑在本地部署业务应用,并通过数据交换与国内相关应用进行对接;在法律法规要求方面,应遵循海外机构所在国家对信息安全、系统建设、海外投资等方面的法律法规要求,对于受法律限制不能在海外机构部署的应用系统,采取国内集中部署策略。对于受法律限制,必须在海外机构部署的应用,采取本地部署策略。在成本方面,需考虑业务应用部署所需投入的资金成本及运维成本,集中部署可共用现有的信息化资源,节省成本,且有利于集中进行系统管理、备份及升级等,节省运维费用。

综合上述因素及系统在实时性要求、标准化程度等方面考虑,可将实时性要求较强的电网运行管理等应用、标准化程度不高的电网营销管理等应用及当地网络环境较差的电源生产管理等应用考虑采取本地部署策略,其余专业类应用与通用类应用可考虑采取集中部署策略。

因此,信息网络建设方面,可优先考虑外网通道的建设。国家电网公司依据“分区、分域、分级”的原则,

将信息系统划分为管理信息大区与生产控制大区,并对管理信息大区划分了信息内网与信息外网。根据国际业务应用部署策略,信息网络建设可考虑信息外网业务集中部署区与海外单位的网络互联建设,通道类型可选择当地互联网接入或租用运营商的 VPN 专线。为满足信息安全要求,应严禁在外网通道传输涉及国家秘密及企业秘密的数据,对于不涉及此类的重要业务数据及敏感信息仍需采取加密等措施进行安全防护。随着海外机构的规模及业务需求增加,在建设成本与安全风险的考虑下,进一步论证内网接入的安全性与其可行性,考虑是否接入公司信息内网。

2 信息安全防护模型

根据电网企业建立的等级保护纵深防御体系,国际业务应用不涉及对国内生产控制系统的直接接入及交互。对于电力系统信息安全研究,在互联电力信息系统方面,需重点关注系统间网关设备安全、电力信息安全 PKI 基础设施的建设;在安全管理方面,加快电力系统信息安全相关标准集的建设及预警、响应和恢复等过程的管理^[1]。

国际业务信息安全防护总体原则需遵循“涉密不上网,上网不涉密”的原则,在终端安全方面,遵循办公计算机信息安全和保密管理的规定,严禁在连接互联网的计算机上处理、存储涉及国家秘密和企业秘密的信息;在网络传输方面,涉及国家秘密和企业秘密信息的传递应遵守国家保密局相关法律法规的规定,严禁在信息内外网传输涉及国家秘密的信息,严禁在信息外网传输涉及企业秘密的信息;在应用与数据交互方面,外网交互内容须经相关职能部门与业务部门审定,并加强外网交互内容安全审计与防护。

如图 1 所示,国际业务信息安全防护模型主要包括主站层、网络层及终端层三个层次。

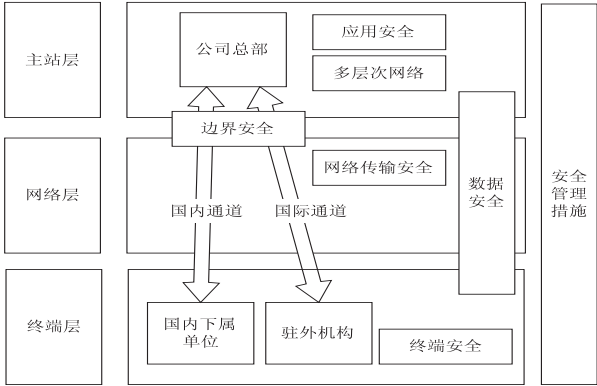


图 1 国际业务信息安全防护模型

主站层安全包括系统应用安全、主站网络层次化防护、主站边界安全接入、主站业务数据保护等;网络层安全主要包括网络数据传输时的加密、认证等措施;

终端层安全主要包括国内下级单位及海外机构办公计算机使用及数据安全。数据安全保护与监控始终贯穿于三个层次。由于国际业务信息化策略主要考虑集中部署策略,对于在个别海外单位本地部署的业务应用,可参照主站系统应用安全、边界安全进行安全防护。同时,信息安全防护模型中参照国际国内信息安全管理标准与体系,建立了相关的安全管理措施。

3 安全技术措施

3.1 主站层安全

主站层安全主要体现在主站网络隔离、边界安全、应用及代码安全、数据保护与监控几个方面。

多层次网络方面,需重点保护信息内网核心业务数据安全,防止敏感信息泄漏,实现信息内外网数据安全隔离交换。网间安全隔离可采用基于可信计算技术的隔离方案,采用标签识别、身份认证、网络隔离技术、虚拟化 Web 服务技术等实现内外网络的可信通信与传输^[2]。电力系统信息内外网安全隔离与数据交换采用基于代理的信息网络安全隔离装置,采用专用的应用服务器访问数据库服务器的安全交互协议与自学习数据库 SQL 注入防护技术实现对数据库的统一隔离防护^[3],如图 2 所示。

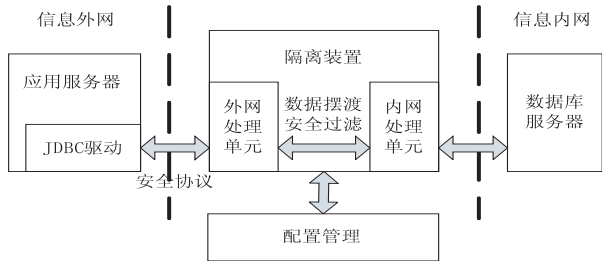


图 2 SQL 代理隔离装置逻辑示意图

此外,在实现 SQL 代理隔离的基础上,针对非结构化数据(例如,电子文档)在内外网间的安全交换,为防止内网敏感数据的泄漏,可采用基于标记的非结构化数据内容过滤技术。以电子文档标记为例,可包含以下信息:用户 ID、文档分类 ID、加密存储的密码、关键字、文档摘要等。通过对电子文档标记的解析与分析,验证文档的完整性、验证文档分类信息的正确性和用户对文档的访问权限及通过关键字判断是否允许文档从安全级别高的网络传送到安全级别低的网络。

边界安全方面,信息外网边界除了部署防火墙、网页防篡改系统、防 DOS/DDOS 攻击设备等安全设备外,需主要关注国内下属单位与海外机构在外网业务访问与数据交互过程中涉及重要业务数据或敏感信息时的双因素身份鉴别与数据加密措施,同时加强边界入侵检测与防御,以应对互联网常见攻击。如在国际业务发展后期考虑建设内网互联通道,海外机构需采

取高安全级别的 SDH 专线等网络通道接入公司总部信息内网,同时在公司总部信息内网边界需采用电力专用安全接入系统实现终端接入的强身份认证、数据隔离交互、数据安全监测与安全检查^[4]。

应用及代码安全方面,除了应用系统提供的身份鉴别、敏感信息加密存储、传输等安全功能外,需主要关注国际业务应用系统或应用模块的代码安全。软件的可靠安全关注于提高软件自身的健壮性,以降低软件自身错误可能引发的安全风险,可靠安全从软件自身缺陷出发,是提高软件安全性的根本途径,检测并修复出软件自身中如缓冲区溢出等缺陷,可以抵御多种病毒与网络攻击^[5]。应用程序的恶意代码防范要求在应用程序上线使用前进行漏洞检测与黑白盒测试等,以防范程序中插入的恶意代码或后门,确保应用程序中不存在恶意代码可利用的漏洞^[6]。

数据保护与监控方面,需关注国际业务数据在主站、网络及终端等方面的安全保护策略部署及安全监控。数据泄漏防护(DLP, Data Leak Prevention)作为信息安全领域的热点之一,其实现途径之一可以采用基于可信计算的安全数据承载平台、扩展的访问控制机制、密钥管理机制、自适应安全策略管理等技术^[7]。针对软件运行过程中产生的临时文件可能发生的数据泄漏问题,可采取动态隔离文件系统对软件进程进行监控,并对需保护的临时文件重定向到保护区域中^[8]。

数据安全作为贯穿三个层次的安全技术手段,其部署方式也应覆盖这几个层次。如图 3 所示,统一数据保护与监控系统主要包括数据保护安全监控系统、数据保护安全管理系统,网络数据安全监测模块、终端数据安全监测模块及其他可扩展的安全监测模块。

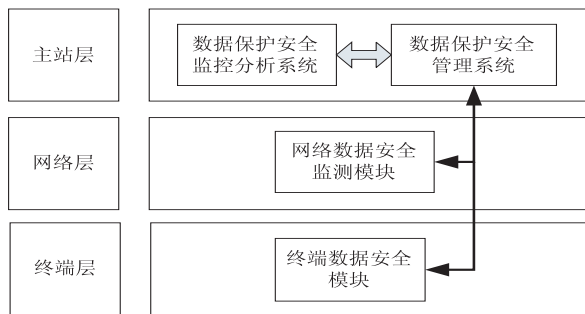


图 3 数据保护与监控系统逻辑示意图

数据保护安全监控分析系统包括业务数据安全监视、数据安全合规监视、数据操作事件监视、数据泄漏趋势分析等模块,实现对终端、业务应用、网络边界、数据库中的数据安全事件、操作审计、安全合规等行为和状态的监视。同时安全策略管理模块负责配置与下发数据安全保护策略。

数据保护安全管理系统包括终端和数据资产管理

模块,负责配置终端、数据库、网络边界数据安全保护策略(例如,加密策略、授权策略等)并进行下发至本地终端数据安全模块、数据库安全模块及网络数据安全监测模块,并收集业务系统、数据库、终端、网络边界的数据安全状态,进行数据操作审计。

3.2 网络层安全

网络层安全主要关注国际业务重要业务数据及敏感数据在网络传输中的保密性、完整性及可用性。数据保护与监控系统中的网络数据安全监测模块实现对网络边界传输的文件或数据安全审计及控制。网络传输数据安全主要通过采用安全协议的 VPN 技术实现身份鉴别、网络传输数据加密、完整性验证等保护措施。应用较为广泛的是 IPSec VPN 与 SSL VPN 技术。

IPSec 为第三层(网络层)隧道协议,广泛应用于公共网络的安全传输。IPSec 中的验证头(Authentication Header, AH)提供了数据源身份验证、数据完整性验证及抗重放攻击的功能,植入安全载荷(Encapsulating Security Payload, ESP)提供了 AH 的安全功能及数据加密功能。基于 IPSec 的 VPN 技术具有灵活性、应用广泛性及通道分离性等特点,其实际应用一般通过端到端配对的 IPSec VPN 网关(例如,总部部署一台网关,海外机构或下属单位部署一台网关)实现端到端的数据传输安全^[9]。

SSL 为传输层与应用层之间的隧道协议,包括握手层协议与记录层协议。SSL 提供了用户端与服务器端的双向身份认证、数据加密、数据完整性保护等功能。SSL VPN 技术具有部署灵活方便、访问控制细化、远程接入方便等特点,其实际应用可通过在总部(主站层)边界部署 SSL VPN 接入平台或网关设备,国内下属单位或海外机构用户通过远程 SSL VPN 拨号与网关建立 VPN 隧道,从而进行安全访问及数据安全传输^[10]。

3.3 终端层安全

如前文所述,在国际业务信息化策略中,业务应用部署原则上尽量考虑集中部署策略。因此,对于国内下属单位及海外单位国际业务信息安全防护的重点主要关注终端安全及终端数据安全。

终端安全方面,一方面,对于国内下属单位,由于信息内网互联的建设较为完善,因此可按公司要求采取通用的终端防病毒、防外联、安全监控等措施。而信息外网暂时未实现全范围的互联,信息外网终端除防病毒、安全监控等措施外,在访问重要国际业务应用时,需加强身份鉴别的措施,例如安装软证书或采用移动硬证书,同时注意对重要业务数据或敏感信息的加密,数据加密可以通过网络层次的 VPN 技术实现;另一方面,对于海外机构终端,访问信息外网的海外终端

安全措施可以参照国内下属单位外网终端的安全防护。而接入信息内网的海外内网终端,由于网络环境与终端使用环境较为复杂,在终端使用、操作等方面需采取更为严格的安全措施。内网终端接入前可对终端主机运行环境进行可信性判断,通过安全接入系统终端计算机环境进行检查和修复,例如,终端系统漏洞检测与修复、终端防病毒软件检测等,对终端进行身份鉴别和安全评估后,如满足接入要求,才允许其接入内网^[11]。因此,海外机构信息内外网终端接入均可通过公司信息内外网边界安全接入或交互平台系统进行终端环境安全检查、终端安全监控及安全接入身份鉴别等安全措施。

终端数据安全方面,可采用终端文档访问与操作权限控制、文档操作审计、文档加密保护、防拷贝、动态实时内存保护、数据备份与恢复等技术措施^[12]。如在前文“主站层安全”中所述,在主站层部署数据保护安全分析系统与安全管理系统,并对终端数据安全模块下发安全策略,终端数据安全模块实现文档加密、权限控制、外发控制、水印保护等功能。

4 安全管理措施

加强信息系统的全生命周期安全管理作为一项重要的信息安全保障措施,在国家电子政务发展过程中,要求加强信息系统建设阶段的安全管理、开发阶段的安全设计及运维阶段的安全管理等^[13]。基于生命周期建立信息安全管理体系统,可将信息安全建设和管理的生命周期分为调研策划、风险评估、设计实施和运行改进等几个阶段,以风险管理为核心,以安全技术为支撑,通过四阶段建立信息安全管理体系统^[14]。

国际业务信息安全管理同样需重点关注国际业务应用系统的全生命周期安全管理。如图 4 所示,国际业务应用生命周期安全管理主要从规划、可研、需求、设计、开发、测试、实施、运行和下线几个阶段采取安全规划、风险分析、方案设计、开发管理、测试管理、上线管理、运行监控与审计等安全管理措施。

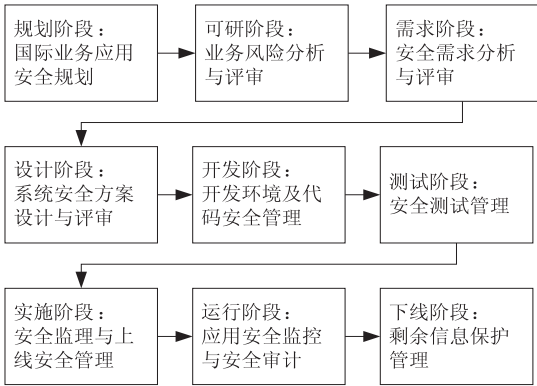


图 4 国际业务应用全生命周期安全管理

此外,可以从以下几个方面采取安全管理措施,加强国际业务信息安全管理:

物理安全:针对可能在海外机构本地部署的业务应用,需加强机房的安全管理,采取安全区域划分、机房出入管理、安全监控及防火、防水、防盗、防破坏、电力供应保障等措施。

办公计算机安全管理:重点关注海外机构的办公计算机使用安全,采取计算机领用登记备案、建立计算机使用安全责任人、计算机设备维护管理、计算机安全监控管理、数据备份与恢复管理等措施。

网络安全管理:对于境外范围建设的网络环境,需采取网络资源管理、网络安全配置管理、网络访问管理、安全审计、网络设备维护管理等措施。

人力资源安全管理:对于从事国际业务的员工,特别是派驻海外机构的员工,采取人员录用考察、人员在职信息安全教育与培训、人员离职审核与保密教育等措施。

用户访问控制管理:主要包括用户访问控制策略管理、访问权限申请与审批、用户口令管理、远程工作管理与控制等措施。

恶意软件防范管理:采取恶意代码防范措施管理、安全漏洞检测与防护管理等措施。

介质安全管理:对于使用的移动存储介质,采取专用安全移动介质领用审批及登记、一般移动存储介质安全检查、介质使用、保存、废弃管理等措施。

第三方服务管理:对于国际业务系统的第三方服务机构,特别是国外的服务机构,需采取安全服务资质审核、能力评定、服务监督管理、服务的监控与评审、服务变更管理、外来人员管理等措施。

业务连续性管理:采取国际业务连续性和影响分析、业务连续性管理计划及计划的测试与评审等措施。

信息安全事件管理:对于国际业务应用及信息化设施可能发生的安全事件、事故进行定义,制定信息安全事件报告、处理、调查与纠正、应急响应等安全管理措施。

知识产权管理:采取知识产权控制策略(例如,保留各类软件所有权证书等证明和证据)、合同中对于知识产权的保护、自开发系统源代码知识产权保护等措施。

法律法规合规性管理:需重点关注海外机构所在国家对于信息系统、信息安全技术、电力信息安全保护等方面的法律法规要求,采取法律法规适用性评价、符合性评价、法律法规传达与培训、更新等安全管理措施。

5 结束语

文中在分析电网企业国际业务信息化策略及风险的基础上,提出了一种三层信息安全防护模型,并对模型各层次关注的关键信息安全技术进行了分析和描述。同时,针对国际业务的特点,提供了信息安全管理思路与相关措施。

随着电网企业国际业务信息化建设的逐步开展,需根据具体业务模式,分等级分类型地同步进行信息安全建设,保障业务数据安全,虽然文中基于电网企业的国际业务信息化及信息安全特点进行研究,但其安全模型不仅对电网企业具有参考与指导意义,同样对其他开展国际业务的企业具有一定的参考意义。

参考文献:

- [1] 李文武,游文霞,王先培. 电力系统信息安全研究综述[J]. 电力系统保护与控制,2011,39(10):140-147.
- [2] 黄胜召,赵辉,鲍忠贵. 网间安全隔离技术分析研究[J]. 通信技术,2010,43(5):100-102.
- [3] 秦昊,林为民,张涛. 基于代理的信息安全网络隔离装置的研究与实现[J]. 计算机与数字工程,2012,40(10):110-112.
- [4] 秦超,张涛,林为民. 电力移动作业PDA安全接入系统设计与实现[J]. 电力系统自动化,2012,36(11):82-85.
- [5] 张立勇. 软件源代码安全分析研究[D]. 西安:西安电子科技大学,2011.
- [6] 李向东,刘晓,夏冰,等. 恶意代码检测技术及其在等级保护工作中的应用[J]. 信息安全,2012(8):164-166.
- [7] 彭维平. 基于可信平台的数据泄漏防护关键技术研究[D]. 北京:北京邮电大学,2011.
- [8] 马俊,王志英,任江春,等. DIFS 基于临时文件隔离实现数据泄漏防护[J]. 计算机研究与发展,2011,48(Sup):17-23.
- [9] 王凤领. 基于IPSec的VPN技术的应用研究[J]. 计算机技术与发展,2012,22(9):250-253.
- [10] 董辉,于润桥,沈翀. SSL VPN隧道技术研究与应用[J]. 微型机与应用,2012,31(24):54-57.
- [11] 杨国利,代祥,毛捍东. 内网终端安全检查与接入控制的设计与实现[J/OL]. 2012. <http://www.cnki.net/kcms/detail/11.2127.TP.20120116.0928.075.html>.
- [12] 张倩红,陈雪华,马传国,等. 基于网络环境的计算机终端数据安全防护研究[J]. 电力信息化,2011,9(11):84-87.
- [13] 周玉建. 信息安全对推进电子政务发展影响分析[J]. 中国科技论坛,2011(9):116-120.
- [14] 于新辉,张建,李伟涛. 基于生命周期分析信息安全管理体[J]. 计算机技术与发展,2012,22(3):237-239.

一种国际业务信息安全防护模型

| | |
|----------|--|
| 作者: | <u>蒋诚智, 刘婷婷, 余勇, JIANG Cheng-zhi, LIU Ting-ting, YU Yong</u> |
| 作者单位: | <u>蒋诚智, 余勇, JIANG Cheng-zhi, YU Yong(中国电力科学研究院 国家电网公司信息网络安全实验室, 江苏 南京, 211106), 刘婷婷, LIU Ting-ting(南京工程学院 通信工程学院, 江苏 南京, 211167)</u> |
| 刊名: | <u>计算机技术与发展</u> |
| | <div>ISTIC</div> |
| 英文刊名: | <u>Computer Technology and Development</u> |
| 年, 卷(期): | <u>2014(1)</u> |

本文链接: http://d.wanfangdata.com.cn/Periodical_wjfz201401041.aspx