C 银行新一代 OA 系统及网络安全体系研究

孙树刚，左琳琳，杨鹏飞，段毅然，赵艺子
（中软信息系统工程有限公司，北京 102209）

摘　要： 基于新一代 IT 技术成果，C 银行建设了新一代办公信息系统（OA2），该 OA 系统具有基础软硬件全国产化、云端一体的系统架构、众创开发持续集成的开发模式、多维智能的纵深防护体系等特点。对该办公信息系统的设计开发、系统结构、安全防护等方面的经验和成果进行总结研究，研究成果能够为相关行业和领域的关键信息基础设施及网络安全建设提供有益的参考和借鉴。

关键词： 新一代 OA 系统；新一代 IT 技术；网络安全；云平台
中图分类号： TP309；F83　　**文献标识码：** A　　**DOI：** 10.19358/j.issn.2097-1788.2022.06.001
引用格式： 孙树刚，左琳琳，杨鹏飞，等. C 银行新一代 OA 系统及网络安全体系研究[J]. 网络安全与数据治理，2022，41(6)：3-9.

Research on the new generation OA system and network security mechanism of Bank C

Sun Shugang，Zuo Linlin，Yang Pengfei，Duan Yiran，Zhao Yizi
（CS&S Information System Engineering Co.，Ltd.，Beijing 102209，China）

Abstract： Based on the latest IT technology development achievements，Bank C has built a new generation of office information system（OA2）. The OA system has the following characteristics：domestic software and hardware，architecture based on cloud and terminal，developing mode based on crowd development and continuous integration，multi-level and intelligent protection system，etc. This paper summarized and studied the experience and achievements in design and development，system structure，security protection and other aspects of the office information system. The research results can provide useful reference for the construction and maintenance of related key information infrastructures and their network security.

Key words： new generation OA system；new generation IT；network security；cloud platform

0 引言

为积极落实信息系统替代升级战略，更好地满足用户对办公信息系统的新需求，C 银行基于以“国产飞腾 CPU 芯片+国产麒麟操作系统”为核心的新一代 IT 技术成果，搭建网络隔离、安全可靠的商密网基础环境，移植现有 OA 系统中成熟功能，开发具有收文、发文、签报等为一体的新一代国产商密办公自动化系统（OA2 系统），实现商密文件电子化全过程管理，为全行商密文件运转和传输提供安全平台和通道，实现全国产化，同时全面提升安全防护能力。OA2 系统是一个安全可靠、体验友好、兼容适配、灵活部署的办公及业务应用支撑平台，也是一个支持信息系统持续众创发展的应用生态服务环境。同时，系统坚持“安全即服务”的原则，打造金融级、智慧型、主动型的网络安全保障体系，为系统运行及应用服务提供灵活、便捷、弹性伸缩、按需分配的网络安全服务[1-2]。本文对该平台的架构、组成、部署应用、网络安全机制等进行研究，期望能够对相关领域产业和技术的发展起到抛砖引玉的作用。

1 系统的总体设计

1.1 系统的构建基础：新一代 IT 技术

随着国内云计算、人工智能、物联网、移动通信、大数据等技术的快速发展及应用，新一代 IT 技术的内涵主要呈现以下几个方面的特点：一是不断完善的国产化生态；二是云端一体的系统架构；三

是支持众创集成的开发模式;四是立体智能的安全防护机制等[3]。

当前,随着新一代 IT 技术的快速发展和用户需求的不断嬗变,过去若干年来基于传统开发模式和系统架构建成的办公信息系统,整体上都面临升级换代的压力。首先,随着信息安全在国家总体安全体系中的地位日益凸显,国家重点行业信息系统和关键信息基础设施的国产化任务日趋紧迫;其次,新一代 IT 技术群的快速发展和应用,也使得用户对许多新型办公应用模式产生了期待。与此同时,面对信息系统生命周期的不断轮回,用户普遍厌倦了过几年全部推倒重来的系统建设模式。面对新的挑战和机遇,必须提出蕴含新技术、新模式的新型解决方案。为贯彻落实网络强国战略,促进央企高质量发展,更好地满足用户对现代办公模式的新需求,C 银行先行先试,基于新一代 IT 技术成果,充分利用国产化软硬件适配成果,成功建设了新一代办公信息系统(OA2),实现了信息化建设的换代升级和国产化,为创新智慧银行服务和构建智慧安全体系提供了系统支持。该办公信息系统基于"网-云-端"架构设计,能够软件硬件一体化直接交付使用,支持众创发展和持续集成,在满足用户办公需求的同时,也为信息系统的替代升级提供了一整套科学的解决方案。

1.2 系统的总体架构:办公云平台

从系统的总体架构看,C 银行新一代办公信息系统是一个基于容器技术的轻量级云平台,该办公云平台面向办公业务应用需求,提供一套专业、简单、灵活、稳定、安全、易用的安全可靠云解决方案。平台主要有以下几个方面的特点:一是屏蔽底层硬件复杂度,为用户提供清晰、简单的配置和监控服务,用户只需要关心业务容量即可;二是屏蔽软件复杂度,构建应用基座,为用户提供完备的应用即插即用服务,用户只需关注要用哪些应用即可;三是为应用互联提供桥梁,为应用提供统一的鉴权、消息、数据服务等;四是构建开放式众创众筹的应用商店,平台提供应用规范及接口标准,应用开发商只需关注业务应用;五是屏蔽客户端软硬件兼容的问题,为用户提供统一的办公桌面,用户操作简单平易;六是兼容原有应用系统,保证应用无缝平滑过渡。

1.3 系统的技术架构:网-云-端模式

系统的技术架构采用典型的"网-云-端"技术路线设计,总体技术架构如图 1 所示。

网为资源层:为系统提供安全可靠硬件网络设施以及基础运行环境,主要是新型的基础设施,包括用户网络和数据中心中的国产的计算设备、存储设备和网络设备等,以及安装在计算机中的基础软件。

云为服务层:主要提供各种云服务,包括云服务三种典型方式:基础设施服务 IaaS、平台服务 PaaS 和软件服务 SaaS,提供众创众筹应用商店功能。

(1)基础设施服务:通过虚拟化技术,形成计算资源池、存储资源池、网络资源池;利用云管理平台实现计算、存储、网络等资源的运行管理与服务调度。

(2)平台服务:包括办公基础服务、办公生态服务等。办公基础服务包括办公服务框架、办公服务接口和办公应用容器,为办公应用的统一访问、权限控制、应用集成接入提供支撑;办公生态服务(应用商店)为应用的入库、分发、部署、卸载、调度提供全面支撑。

(3)软件服务:基于平台,定制开发首页、收文管理、发文管理、签报管理、便函管理、待办事宜、个人办公、电子档案管理、业务配置管理、系统管理等功能服务。

端为应用层:为用户提供个性化的应用,一般是为用户量身定做的各种办公应用,包括系统业务用户、业务管理人员、系统管理人员、系统运维人员等,可根据各级单位使用权限配置应用功能。

2 系统的安全防护机制设计

2.1 安全防护需求分析

基于自主化基础软硬件平台,新一代 OA 系统综合运用身份认证、安全拦截策略、文件商密标识及加密等技术,进行安全保密一体化设计,全面提升安全防护能力。参照《信息系统安全等级保护基本要求》(GB/T 22239-2008)、《信息系统安全等级保护测评要求》(GB/T 28448-2012)、《中央企业商业秘密保护暂行规定》《中央企业商业秘密信息系统安全技术指引》等要求,结合 C 银行信息系统安全保密相关标准规范和管理规定,以商密文件全生命周期管理为目标,新一代 OA 系统需要对商密文件处理的每个环节进行安全保密防护。OA 系统安全防护主要需求如表 1 所示。

2.2 网络安全部署架构设计

针对安全防护建设的需求,系统划分不同的安全域,做出相应的安全防护设计,在不同的安全区

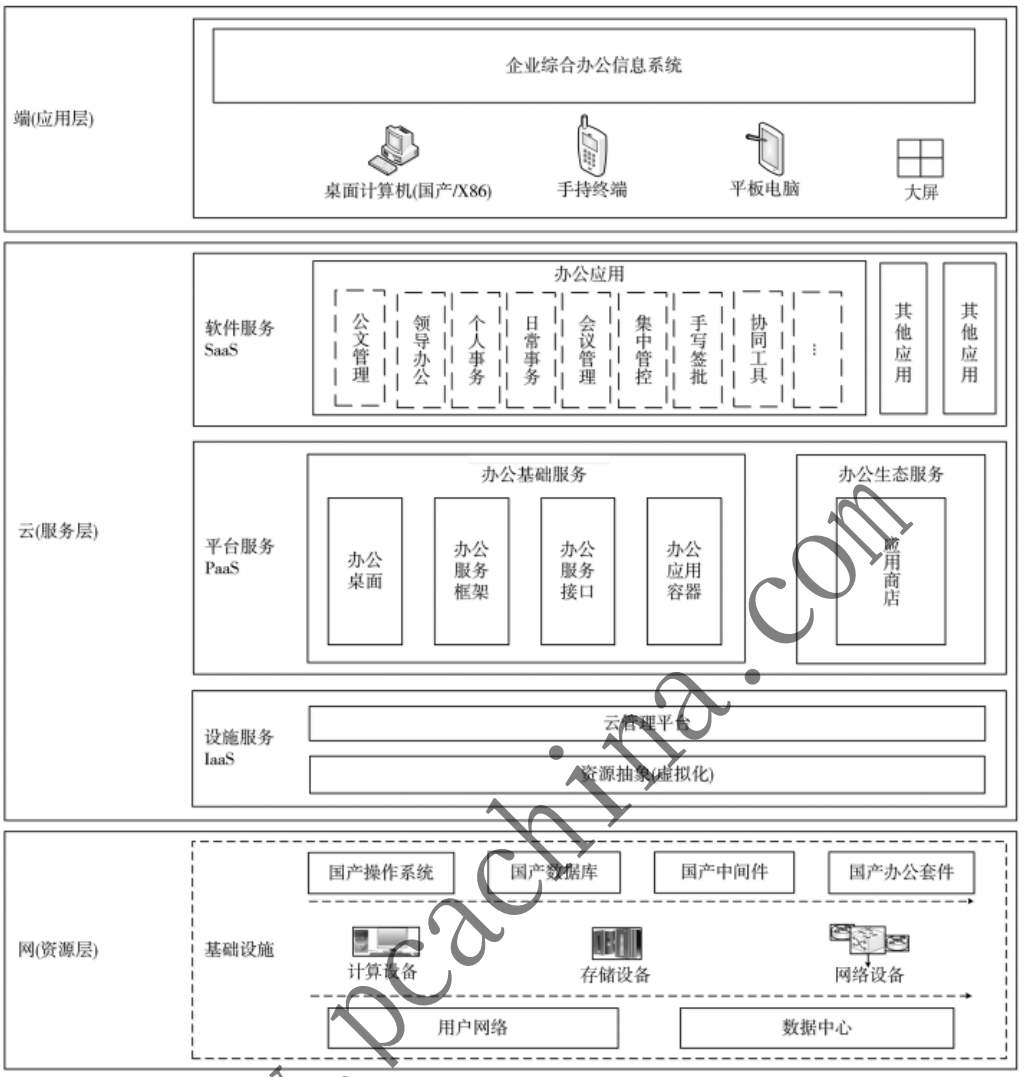


图 1 系统总体技术架构图

表 1 网络安全防护需求

安全类型	安全防护需求
物理安全	1、安全防护设备需选用经过国家授权部门认可的产品； 2、机房应采取相应的防火、防雷击、防水防潮等相关措施
网络安全	1、商密办公网与其他网络实施逻辑隔离，依托公共网络信道跨区域传输信息应具有数据加密措施； 2、根据业务需求、网络结构、安全保密防护能力的状况划分不同的逻辑域或分区，进行隔离和访问控制； 3、应具有网络事件审计记录功能，审计日志应至少保留 60 天； 4、应具有对违规事件进行监视、报警和控制处理的措施； 5、应能够对设备接入进行控制，对用户违规接入行为进行监控
主机安全	1、应具有禁止非法外联、文件数据保护、外设使用监控等终端防护措施； 2、禁止安装与工作无关的应用软件，关闭不需要的系统服务； 3、应及时安装相应安全补丁程序； 4、应安装防病毒软件并及时升级； 5、应采用双因素认证或生物特征认证
数据安全	1、办公业务数据需带商密标识，具有数据存储保护功能； 2、应具有数据本地备份功能； 3、应具有信息输入输出控制，制定信息输出策略和流程并保留审计记录

域分别部署相应的安全设备,保证网络、数据及各业务应用的安全;平台需要基于国产化体系,构建支撑平台系统运行的网络和数据中心系统基础设施,部署专用机服务器和国产自主安全可靠数据库、中间件、存储等基础软硬件。

边界防护区域:在边界防护区域部署了抗泛洪攻击、恶意代码检查、链路负载、防病毒过滤、防火墙、VPN 等设备,实现对外来访问的防护和管理;通过部署 NAT 与 ADS-M 识别核心资产,设置 DDoS 防护策略,全天候检查业务异常,及时响应和拦截 DDoS 攻击等四个步骤完善 DDoS 的防护体系,提供强大的安全防护止损能力,在安全运维管理域部署日志审计与态势感知系统,通过对各个安全产品日志收集、SNMP 监控等技术,实现对产品链路、日志、状态等的实时监控。

核心交换区:在核心交换机部署万兆安全防火墙设备,来保证业务网之间的安全访问管控、业务逻辑隔离。核心网络之间信息的传递数据量很大,设备之间采用 40 G 互联。部署 IDS 来监控网络中的入侵攻击行为,并发出报警,同时按照预定的响应规则对攻击事件作出响应, 核查系统漏洞及后门,协助管理员加强网络安全的管理。通过部署网络审计系统,与其他网络安全设备进行联动,将各自的监控记录通过安全管理中心, 集中对网络异常、攻击和病毒进行分析和检测。

云业务应用区:为保证业务系统的安全运行,在业务应用区配置防火墙。同时,为保证虚拟边界安全,部署云安全套件,实现虚拟边界的访问控制、入侵防范和恶意代码控制,并保证策略随主机迁移。

DMZ 区(数据交换区):为保证服务网站的安全,部署网页防篡改系统与应用负载,对 Web 文件内容实时监控与恢复,为门户网站提供实时自动安全监护。

数据存储区:为保证数据信息的安全,需要配置数据库审计设备,以便能够实时记录网络上的数据库活动,对数据库操作进行细粒度审计的合规性管理,对数据库遭受到的风险行为进行告警,对攻击行为进行阻断。(部署云安全套件,实现虚拟边界的访问控制、入侵防范和恶意代码控制,并保证策略随主机迁移。)

用户终端区:为保证信息及用户终端的安全,需要在用户终端上部署防病毒软件客户端。

安全运维管理区:在运维管理区部署堡垒主机,进行统一的身份鉴别和操作行为审计,进行统一的身份管理,拦截非法访问和恶意攻击,对不合法命令进行阻断,过滤掉所有对目标设备的非法访问行为;在运维管理区配置漏洞扫描设备,通过漏洞扫描系统及时找出网络中存在的隐患和漏洞,帮助用户及时修补漏洞,保障网络安全事件不对网络造成影响。与原身份认证系统和现应用系统进行访问控制联动,实现对业务、应用访问接入的控制。主机和终端安全是一个综合的系统问题,涉及管理计算机本身、计算机应用、计算机操作者、计算机使用单位规范等多个方面因素,所以需要部署补丁管理系统。部署安全管理平台统一对整个网络安全进行监控、管理和维护。

各网络区域之间用安全边界防护设备及配置相应的访问控制策略进行安全隔离。

2.3 安全防护体系总体架构

新一代 OA 系统采用自主安全支撑平台与 C 银行现有办公化平台进行深度融合,在满足商密办公和普通办公一体化应用的同时,采用安全保密技术手段,保障办公系统安全,并且实现商密公文和普通公文应用和数据的逻辑隔离,保护商密文件安全。面对传统安全威胁和非传统安全威胁,结合等级保护标准要求,系统从安全技术、安全管理、安全运维三个角度构建多维立体安全防护体系,切实保障网络信息安全。系统安全防护体系总体架构如图2所示。

2.4 安全防护技术体系

在安全防护技术体系维度,将系统安全分解到物理、网络、主机、应用和数据等各个层面进行安全措施的落实。系统安全防护技术体系如图 3 所示。

(1)物理安全设计

根据等级保护标准基本要求,系统基础设施设计和建设主要考虑以下因素:环境(防火、防水、防雷击等)、设备和介质等方面的安全。具体包括:物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护。

(2)网络安全设计

系统网络层安全技术体系主要设计了以下安全防护机制:网络结构安全、网络访问控制、网络安全审计、边界完整性检查、入侵防范、恶意代码防

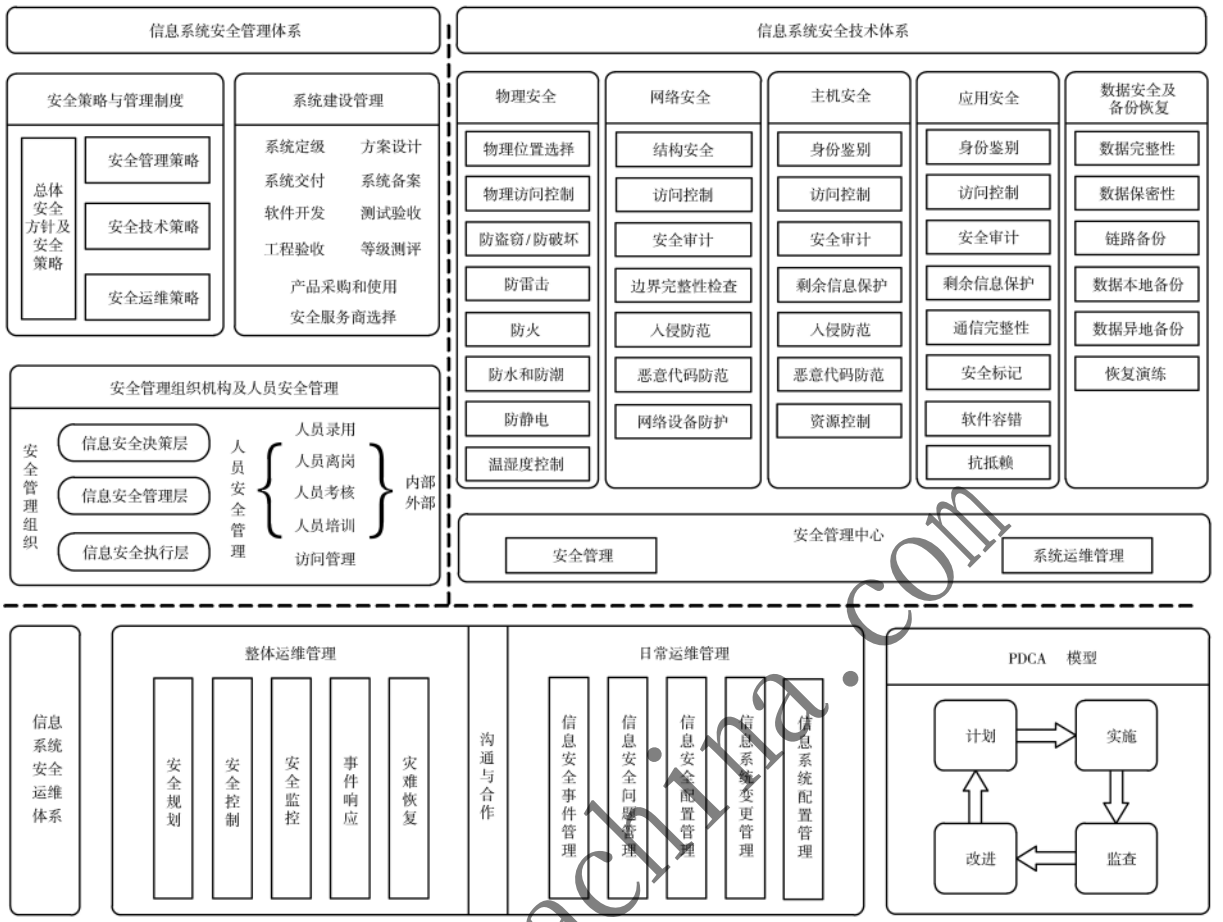


图 2 系统安全防护体系总体架构图

范、网络设备防护等。系统通过在安全管理区部署堡垒机实现对网络设备自身的防护。同时,系统支持单点登录,支持运维过程审计,支持密码自动定期修改等功能。

(3)主机和用户访问安全设计

主机和用户访问安全方面主要设计了身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范、资源控制几大类安全控制机制。

(4)应用安全设计

应用安全方面主要设计了身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性和保密性、软件容错、抗抵赖几大类安全控制机制。

(5)数据安全及备份恢复设计

信息系统处理的各种数据(用户数据、系统数据、业务数据等)在维持系统正常运行上起着至关重要的作用。一旦数据遭到破坏(泄漏、修改、毁坏),都会在不同程度上造成影响,从而危害到系统的正常运行。由于信息系统的各个层面(网络、主机、应用等)都对各类数据进行传输、存储和处理等,因此,数据保护需要物理环境、网络、数据库和操作系统、应用程序等提供支持。

数据备份也是防止数据被破坏后无法恢复的重要手段,而硬件备份等更是保证系统可用的重要内容,在高级别的信息系统中采用异地适时备份会有效地防治灾难发生时可能造成的系统危害。

数据安全和备份恢复机制主要对数据完整性、数据保密性、备份和恢复等几个关键控制点进行了设计。

2.5 商密数据生命周期管理

按照《中央企业商业秘密安全保护技术指引》要求,系统对商密文件全生命周期的每个阶段进行安全防护措施的设计,以数据加密技术为核心,在数据的形成、流转、存储、使用等各阶段,进行商密数据安全防护,保证非密数据自由使用,商密数据安全可控,并最大程度确保不影响用户正常办公。主要采取了以下几个方面的措施:

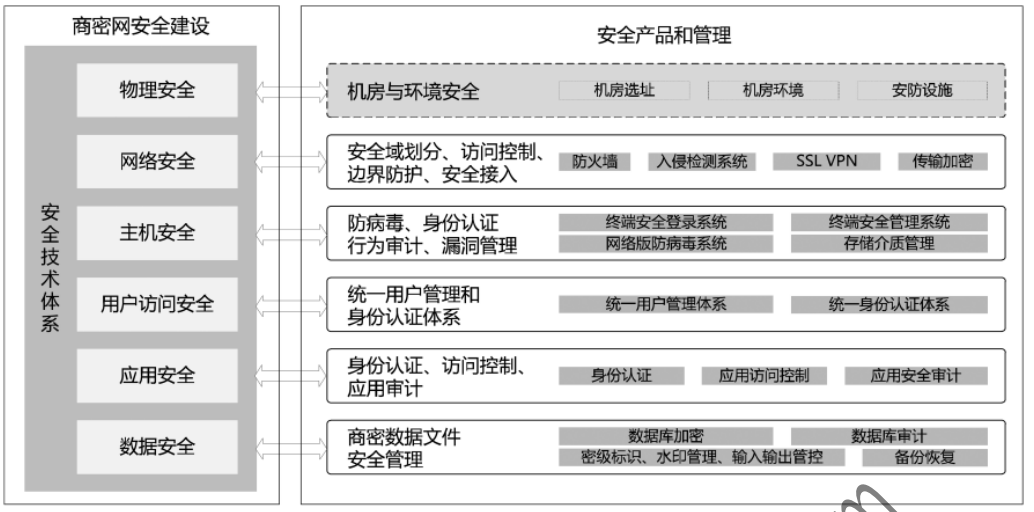


图 3 系统安全防护技术体系

(1)事前加密保护。数据库服务器配置支持国密算法的密码卡,实现数据库透明加密保护;在总行和各级机构终端之间跨域互联部分,采用 SSL VPN 对网络数据进行加密保护;在总行商密办公服务器上部署商密标识应用中间件,与商密办公系统集成,对商密文件加电子标识保护,保证电子标志与电子文件唯一性绑定,不可分离、不可非授权篡改。安全保障区部署商密标识生成和管理系统。

(2)事中权限控制。在商密网核心区域部署终端准入控制系统,实现对终端接入商密办公系统的准入控制;商密办公应用系统采用基于角色的访问控制技术,在身份认证基础上,针对不同用户角色授权不同应用功能;通过基于标识的文件安全管理和基于标识的文件安全控制,实现商密文件权限控制。

(3)全程审计,事后可查。采用网络运维审计系统、数据库审计系统和统一安全管理中心系统,结合应用审计和防火墙、入侵检测等产生的安全事件,从网络接入、办公处理、数据访问到输入输出进行全方位审计。

2.6 安全防护优势

C 银行新一代 OA 系统基于国产化基础软硬件生态建设成果,对网络安全体系进行创新设计,和传统 OA 系统相比,其安全防护优势主要体现在以下几个方面:

(1)系统基于中国电子(CEC)研发的 PKS 安全体系构建网络安全机制。PKS 从内到外实现了八重安全防护机制,分别是:基于飞腾 CPU 芯片的可信计算防护、内存条安全区防护、整机防护、杀毒软件防护、可信运行区防护、系统分析防护、安全运行框架防护、安全管控中心防护。C 银行新一代 OA 系统基于 PKS 的 CPU 内置可信技术、内存内置物理防护技术、终端统一安全中心、云端统一安全管控等成果实现了底层构架的本质安全。

(2)系统基于“安全即服务”的设计理念,实现安全技术体系从功能型到智慧型、灵活型、主动型转变[4]。C 银行新一代 OA 系统构建了企业级安全架构体系,该体系采用面向服务架构、云计算、组件化、可视化开发等技术,将安全功能从应用中解耦,实现安全功能的组件化、标准化和参数化,形成以用户认证、密码服务、安全监控、安全策略管理等安全组件为核心,以近 300 个安全服务为代表的“安全功能库”。所有安全功能由策略管理中心动态调配,可依据所面临的风险智能匹配适用的安全策略,启动相应的安全功能,从而灵活应对已知和未知威胁带来的风险。因为是以服务的方式提供安全功能,办公应用可专注功能开发,无需关注安全服务的具体实现方式。该安全体系有力支撑了 C 银行新一代 OA 系统的安全运行,在保障网络安全可控的同时,实现了非密数据的自由使用[5],也改善了用户体验[6]。

(3)系统改变“木桶式”安全架构体系,将系统安全分解到物理、网络、主机、应用和数据等各个层面进行落实,建立纵深“多层水闸式”的防护体系;同时,系统充分运用威胁情报、大数据分析、智能风控、生物特征识别等技术,建立主动防控体系,基于网络安全态势感知,系统可实时、动态调整安全防

护策略，实现网络安全的智慧防控。

3 结论

C银行新一代OA系统(OA2系统)基于新一代IT技术成果，首次将国产化自主安全软硬件产品规模化、体系化应用于银行系统。通过OA2系统建设，自主进行了IT架构设计，自主建立了IT基础环境，自主设计了系统安全防护架构，自主构建了银行业务新蓝图，实现了预期的技术效益、产业生态效益和网络安全效益。系统进一步优化和升级将紧跟国家战略发展要求，并力争成为同行业国产化平台应用的示范性工程。下一步，C银行将以新一代OA系统(OA2)建设为切入点，聚焦自主安全替代和网信安全优化，从以下几个维度对系统持续完善和升级：

一是基于国产自有的信息技术产品，构建包括“分布式应用、分布式框架平台和底层云基础设施”在内的全栈国产化自主解决方案，形成金融行业通用的一体化解决方案，提升金融行业的技术自主力、服务力。

二是联合相关科技创新型企业及金融机构，共同实现解决方案的验证和落地，为解决方案在行业的应用与推广做出示范。

三是建立联合创新实验室，加强基于国产芯片、操作系统、数据库、中间件等基础软硬件的应用适配攻关，加速国产化技术方案的形成和应用落地。

四是基于金融业标准化体系框架，将长期积累的方法、工艺、规范等业界领先的标准化内容进行提炼，转化为具有行业共性推广价值的行业标准。

五是持续优化智慧安全体系，不断提升安全服务和保障能力。探索建立基于大数据和人工智能技术的主动式安全态势感知模型，主动发现和应对安全威胁，实现更加智能灵活的安全防护。

参考文献

[1] 金磐石.建设银行打造新一代智慧银行[J].中国金融电脑，2017(2)：19-23.
[2] 金磐石.构建智慧安全体系助力金融科技创新[J].中国金融电脑，2017(8)：23-26.
[3] 鲍莹.开展信息安全建设打造银行信息安全四维体系[J].中国金融电脑，2021(1)：72-75.
[4] 丁海虹.具备主动防御能力的建行云安全防护体系[J].金融电子化，2020(7)：76-77.
[5] 刘静芳.增强数据安全责任意识完善数据安全管理体系[J].金融电子化，2021(7)：26-28.
[6] 郭汉利.商业银行信息安全的智慧防控[J].金融电子化，2019(10)：57-58.

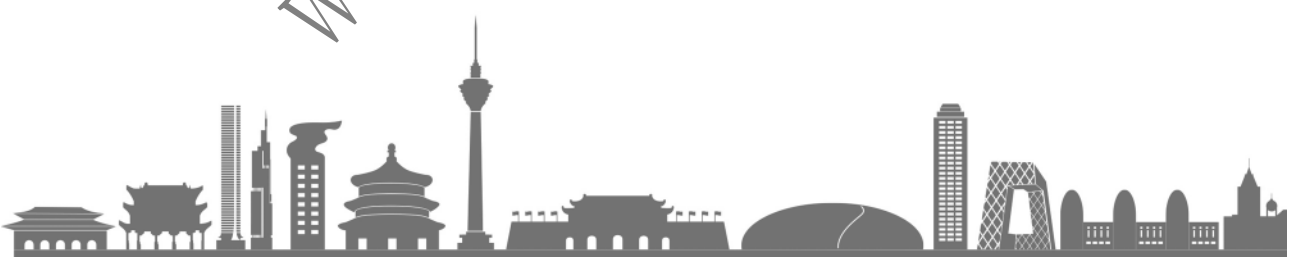
(收稿日期：2022-09-29)

作者简介：

孙树刚(1981-)，男，本科，高级工程师，主要研究方向：网信系统项目管理、办公及业务信息系统、自主可控自态建设、网络安全等。

左琳琳(1977-)，女，工学硕士，高级工程师，主要研究方向：军事信息系统、大数据、人工智能、网络安全等。

杨鹏飞(1985-)，男，工学博士，工程师，主要研究方向：军事通信系统、大数据处理、人工智能等。



版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部