基于商用密码应用的政务信息系统安全加固与风险评估实践

钟明福
广州金网安信息科技有限公司，广东 广州 510000
DOI:10.61369/ME.2025040006

摘　　要： 政务信息系统面临安全威胁，阐述其架构风险，介绍商密技术支撑，如 SM 系列算法等，还涉及防护架构、访问控制模型、评估指标等内容，以及相关实践成效与未来挑战，包括省级政务云平台案例验证等

关 键 词： 政务信息系统；商用密码；安全加固

Practical Practice of Security Reinforcement and Risk Assessment of Government Information System Based on Commercial Cryptographic Application

Zhong Mingfu
Guangzhou Jinnet Security Information Technology Co., LTD., Guangzhou, Guangdong 510000

Abstract: Government information systems face security threats. This paper discusses the architectural risks of these systems, introduces commercial cryptography technologies, such as SM series algorithms, and covers protection architectures, access control models, evaluation metrics, and other related practices. It also examines the practical outcomes and future challenges, including case studies from provincial government cloud platforms.

Keywords: government information systems; commercial cryptography; security reinforcement

引言

随着信息技术的飞速发展，政务信息系统的安全问题日益凸显。2017年颁布的《中华人民共和国网络安全法》强调了保障网络安全的重要性，为政务信息系统安全加固提供了法律依据。政务信息系统面临着数据泄露、身份冒用等多种安全威胁，其架构在数据全生命周期存在风险。同时，复杂的网络环境使系统易受攻击，影响其安全运行。因此，对政务信息系统进行安全加固与风险评估至关重要，商用密码技术等多种手段的应用成为保障其安全的关键。

一、政务信息系统安全风险与商用密码技术基础

（一）政务系统安全威胁特征分析

政务信息系统面临多种安全威胁。通过解构典型政务系统架构，可发现数据全生命周期存在诸多风险。如敏感数据暴露，可能在数据采集、存储、传输或使用过程中发生，导致信息泄露[1]。身份冒用也是常见风险，攻击者可能伪装成合法用户获取系统权限。结合近三年关键基础设施攻击事件统计，能进一步量化系统脆弱性指标。这些攻击事件反映出政务系统在面对复杂网络环境时的脆弱性，如网络攻击可能导致服务中断、数据篡改等严重后果，为政务信息系统的安全运行带来巨大挑战。

（二）商用密码技术体系解析

政务信息系统的安全保障至关重要，商用密码技术是关键支撑。SM系列商密算法具有独特的实现机理，其在加密、解密过程中遵循特定的数学规则和逻辑，确保信息的保密性和完整性[2]。IBC标识密码与PKI体系在适用场景上存在差异。IBC标识密码以用户的标识作为公钥，无需复杂的证书管理，适用于一些对便捷性要求较高的场景；而PKI体系基于证书信任机制，在大规模网络环境和复杂信任关系场景中应用广泛。同时，密码芯片、VPN设备、密钥管理系统等构成了重要的产品技术图谱。密码芯片提供高效的加密运算能力，VPN设备保障网络通信安全，密钥管理系统负责密钥的生成、存储和分发等关键操作，共同为政务信息系统安全保驾护航[2]。

二、基于密码技术的安全加固体系设计

（一）密码应用改造方案设计

面向政务专网设计三层防护架构，网络层采用IPSec通道加

密，确保网络传输的保密性与完整性[3]。通过建立IPSec通道，对网络数据包进行加密和验证，防止数据在传输过程中被窃取或篡改。数据层实施结构化数据脱敏，保护敏感信息。在对数据进行处理和存储时，对敏感字段进行脱敏处理，使得数据在可用性不受影响的前提下，隐私信息得到有效保护。应用层运用数字签名验证，保障应用的真实性和不可抵赖性。同时，设计基于国产密码机的双证书认证体系实施方案，通过颁发不同用途的证书，进一步增强认证的安全性和可靠性。

（二）动态访问控制机制

构建基于属性加密的ABAC模型，可依据主体属性、客体属性以及环境属性进行动态访问控制决策，从而实现数据访问最小授权策略，精准地限制主体对数据资源的访问权限[4]。同时，整合数字证书认证与生物特征识别技术，增强身份认证的准确性与可靠性。通过数字证书验证用户身份的合法性，结合生物特征识别技术进一步确认用户的真实性，避免身份冒用。在此基础上，设计符合GB/T 39786的会话动态鉴权流程，在会话过程中实时验证用户的访问权限，根据用户的操作和系统环境的变化动态调整访问控制策略，确保政务信息系统的安全性和合规性。

三、安全风险评估模型与方法

（一）密码应用有效性评估模型

1.合规性评估指标体系

建立覆盖密码算法、密钥管理、运维管控的二十项三级评估指标，旨在量化测评符合GBT 39786-2021标准要求的满足度。对于密码算法，评估指标可涉及算法的正确性、安全性以及适用性等方面，确保其符合相关标准和规范[5]。在密钥管理部分，指标涵盖密钥的生成、存储、分发、更新和销毁等全生命周期过程，以保障密钥的安全性和有效性。运维管控方面的评估指标则注重对密码系统的日常运行维护、监控和应急处理能力，确保密码应用在政务信息系统中的稳定运行和安全可靠。通过这些全面且细致的评估指标，能够系统地评估密码应用的合规性和有效性，为政务信息系统的安全加固提供有力支撑。

2.风险量化评估方法

融合层次分析法与模糊数学理论构建半定量评估模型。层次分析法可将复杂问题分解为多个层次，确定各因素的权重[6]。模糊数学理论则用于处理评估中的模糊性和不确定性。通过该模型评估威胁发生概率与影响程度。同时，设计带权重的风险矩阵可视化展现方法，以直观呈现风险状况。这种方法将风险的两个关键维度——发生概率和影响程度进行综合考量，并依据权重分配在矩阵中定位风险等级，为政务信息系统的安全加固与风险评估提供科学有效的量化手段。

（二）实战化风险评估实践

1.攻击模拟测试方案

基于MITRE ATT&CK框架，通过设计七类攻击场景来构建攻击模拟测试方案。其中涵盖中间人攻击、密钥破解等专项测试用例，以此模拟真实的攻击情况。这些攻击场景和测试用例的设计旨在全面检验政务信息系统在面对不同类型攻击时的安全性。通过构建红蓝对抗演练验证体系，红方模拟攻击者实施攻击，蓝方则进行防御，在对抗过程中发现系统存在的安全漏洞和风险点，为后续的安全加固和风险评估提供有力依据[7]。

2.残余风险评估模型

建立安全措施有效性系数是残余风险评估模型的关键。该系数能够量化安全措施对风险的控制程度[8]。通过对系统中各项安全措施的分析和评估，确定其在降低风险方面的实际效果。在此基础上，提出风险敞口计算公式。此公式综合考虑了风险发生的可能性、影响程度以及安全措施有效性系数等因素，能够准确地计算出系统在现有安全措施下的风险敞口大小。最后，利用蒙特卡洛仿真方法确定不可接受风险的阈值区间。蒙特卡洛仿真通过大量的随机模拟，能够考虑到各种不确定性因素，从而为风险评估提供更可靠的依据，明确系统中哪些风险处于不可接受的范围。

四、综合防护体系实施与优化

（一）分层安全加固实施

1.基础设施层改造

在基础设施层改造中，对于政务信息系统安全加固至关重要。密码资源池部署架构是关键环节，其架构图展示了核心要点。其中SSL卸载设备集群部署需精心规划，要考虑设备的性能、数量以及与整体系统的兼容性，确保高效处理SSL加密任务，减轻服务器负担[9]。同时，密码中间件适配改造也不容忽视，需根据政务系统的特点和需求，对中间件进行针对性的调整和优化，使其能够更好地与密码资源池协同工作，保障信息在传输和存储过程中的安全性和完整性，从而提升整个政务信息系统的安全防护能力。

2.数据安全防护实施

在综合防护体系的实施与优化中，数据安全防护至关重要。对于政务信息系统，需依据相关标准和要求进行数据安全防护实施。以电子公文传输系统为例，其在国密算法改造过程中，应注重对数据的分层安全加固。在数据库层面，采用基于SM9算法的字段级加密方案，这不仅能保证数据的保密性，还能增强数据的完整性和可用性。通过对数据进行加密处理，可有效防止数据在传输和存储过程中被窃取或篡改，从而确保政务信息的安全可靠，为政务工作的顺利开展提供有力保障[10]。

（二）安全监测体系构建

1.密码设备运行监控

设计密码服务健康度监测指标是密码设备运行监控的重要环节。这些指标应涵盖密码设备的多个关键方面，如加密算法的正确性、密钥的安全性和可用性等。通过对这些指标的实时监测，可以及时发现密码设备运行过程中可能存在的问题。同时，开发可视化监管平台也至关重要。该平台具备证书有效性验证功能，可确保证书在有效期内且未被篡改，保障通信的安全性。密钥生命周期监控功能能够对密钥的生成、存储、使用和销毁等各个阶

段进行严格监控，防止密钥泄露或滥用。通过这样的监测指标和监管平台，能够实现对密码设备运行的有效监控，提升政务信息系统的安全性。

2.异常行为感知系统

应用流密码分析技术构建行为基线模型是异常行为感知系统的关键。通过对政务信息系统中数据的流动及加密解密操作进行深入分析，以正常行为模式为基础建立基线。当出现密钥异常申请时，系统能迅速捕捉该行为与基线的偏离。解密频率突变同样如此，一旦超出设定的合理范围，系统即刻发出预警。针对九类风险，均依据各自的特征在行为基线模型中有相应的判断标准。这种实时预警机制能够有效感知系统中的异常行为，为政务信息系统的安全防护提供及时且准确的信息，保障系统的安全性和稳定性。

（三）持续改进机制

1.周期性评估机制

基于商用密码应用的政务信息系统安全加固与风险评估实践中，综合防护体系的持续改进与周期性评估机制至关重要。需制定密码应用成熟度评价模型，以此为标准衡量系统安全状况。规划半年期的全要素评估与漏洞复测工作流程，全要素评估涵盖系统各方面，漏洞复测确保修复效果。通过这样的流程形成 PDCA 管理闭环，即计划（Plan）、执行（Do）、检查（Check）、处理（Act）。在计划阶段确定评估目标与方法，执行阶段实施评估与修复，检查阶段验证结果，处理阶段总结经验并对后续计划进行调整，不断优化综合防护体系，提升政务信息系统的安全性。

2.应急响应体系

建立密码设备双机热备切换预案是应急响应体系的重要部分。当主设备出现故障时，能迅速切换到备用设备，确保政务信息系统的密码应用服务不中断。同时，针对密钥泄漏这一严重安全事件，设计详细的应急响应流程图。一旦发生密钥泄漏，立即启动包含密钥撤销、系统隔离等六类处置措施的流程。密钥撤销可防止泄漏的密钥继续被使用，系统隔离则避免风险扩散到其他部分。通过这些措施，能够有效应对密码应用过程中的突发安全事件，保障政务信息系统的安全稳定运行。

五、总结

政务信息系统基于商用密码应用进行安全加固与风险评估实践取得显著成效。通过省级政务云平台案例验证，系统密码应用合规率大幅提升，从62%提高到98%，同时残余风险值也降低至可接受范围。这表明相关实践措施在提升系统安全性方面起到了关键作用。然而，随着技术发展，未来仍面临挑战，需关注量子计算带来的潜在威胁，并积极探索密码技术与区块链、隐私计算融合的新发展路径，以进一步增强政务信息系统的安全性和适应性，更好地应对不断变化的安全环境。

参考文献

[1]都彦辰 .S省商用密码使用监管问题及对策研究 [D].山东大学，2023.

[2]缪新建 .Z政务信息系统项目风险管理研究 [D].广东工业大学，2021.

[3]卢赛 .信息系统安全风险评估技术的研究与应用 [D].南京航空航天大学，2021.

[4]谷训刚 .基于机器学习的政务信息系统软件成本估算研究 [D].齐鲁工业大学，2022.

[5]邱子杨 .面向 Android应用安全加固的 smali代码混淆研究 [D].南京邮电大学，2021.

[6]罗文兵，崔宁宁，徐海波 . 浅议基于商用密码技术加固视频监控安全 [J]. 中国设备工程，2022(5):212-213.

[7]黄晶晶，孙淑娴，周睿康，等 . 商用密码应用安全性评估 [J]. 信息安全与通信保密，2023(3):113-121.

[8]陆宙，王文兵 . 医院商用密码应用建设实践 [J]. 电子元器件与信息技术，2023,7(4):191-195.

[9]宫铭豪，丁森华 . 应急广播系统商用密码应用安全性评估研究 [J]. 广播电视信息，2022,29(8):97-100.

[10]白荣华，魏强，郭瑞，等 . 政务信息系统商用密码集约化平台设计与实现 [J]. 信息安全研究，2023,9(5):461-468.

