数字政府建设面临的多重风险及其规避策略

董倩
（辽宁省大数据管理中心<辽宁省信息中心>，辽宁　沈阳　110032）

【摘　要】数字政府是通过数字化技术实现政府职能，提高政府服务效率和质量的一种新型治理模式，随着信息技术的快速发展，数字政府建设已成为现代社会治理的重要方向。然而，在数字政府的建设过程中，面临着多种风险，如信息安全、数据隐私、技术漏洞和网络攻击等。本文旨在探讨数字政府建设中所面临的多重风险，并提出相应的规避策略，以提升数字政府的建设质量和安全性。

【关键词】数字政府；建设风险；规避策略

引言：在数字政府的建设过程中，由于涉及大量的数据和信息，面临着多种风险。这些风险不仅可能对政府服务的质量和安全性产生影响，还可能对国家安全和社会稳定造成威胁。因此，对数字政府建设中的多重风险进行深入分析，并提出相应的规避策略具有重要意义。

一、数字政府建设的必要条件

首先，数字政府建设需要建立完善的组织架构，包括领导机构、技术团队、业务团队等，明确各部门的职责和分工，实现跨部门、跨层级的协同管理。同时，数字政府建设需要采用先进的数字化技术，包括云计算、大数据、人工智能、区块链等，以实现数据的高效处理、分析和利用，提高政府服务的质量和效率。

其次，数字政府建设需要具备丰富的数据资源，包括政务数据、社会数据、经济数据等，以提供决策支持和公共服务所需的数据支持。同时，数字政府建设需要与相关部门和机构建立良好的合作关系，包括政府部门、科研机构、企业等，共同推进数字化建设和公共服务创新。当然，数字政府建设还需要具备充足的人才储备，包括技术人才、管理人才、业务人才等，以提供数字化建设和公共服务所需的人才支持。

最后，数字政府建设需要建立完善的信息安全保障体系，包括网络安全、数据保护、隐私保护等，确保数字政府建设和公共服务的安全性和可靠性。同时，数字政府建设需要可持续的投入和支持，包括资金投入、政策支持、社会参与等，以提供数字化建设和公共服务的长期保障和支持。

二、建设数字政府的核心能力

（一）数据治理与整合能力

建设数字政府需要制定统一的数据标准和规范，确保各部门、各系统之间的数据格式和定义一致；有效清除重复、无效和不准确的数据，将不同来源的数据整合到一个统一的数据平台；制定并执行严格的数据安全和隐私保护政策，防止数据泄露、篡改和滥用。同时，构建一个中心化的数据交换平台，支持各部门之间的数据实时共享和交换；打破数据孤岛，通过技术手段和管理措施，消除部门之间的数据壁垒，实现数据的跨部门流通。提供统一的数据访问接口，使得不同的系统和应用都能够方便地获取和使用数据。

（二）数据分析能力

构建能够处理海量数据的分析平台，支持实时数据流处理和批量数据处理。掌握和应用机器学习、深度学习等先进的分析算法，对数据进行深度挖掘和预测分析。提供直观易用的可视化分析工具，帮助分析人员更好地理解和解释数据。

（三）数据可视化能力

将数据以图表、地图、仪表板等形式进行可视化设计，使得数据更易于理解和解读。提供交互式的数据分析工具，允许用户动态地查询和探索数据，发现数据中的规律和趋势。

（四）数字化服务能力

建设多样化的在线服务渠道，如政府网站、移动应用、社交媒体等，方便公民随时随地进行服务申请和咨询。通过数字化手段优化服务流程，减少办事环节和时间，提高服务效率。

引入智能客服系统，通过自然语言处理和机器学习技术，实现自动化的服务咨询和问题解答。

（五）信息安全保障能力

加强网络基础设施的安全防护，防范网络攻击、病毒传播等安全风险。对重要数据进行加密存储和定期备份，确保数据的机密性和完整性。建立应急响应机制，对安全事件进行快速响应和处理，减轻安全事件的影响。

三、数字政府建设面临的多重风险与应对策略

（一）信息安全风险与应对策略

1. 数据泄露风险

数字政府建设过程中，涉及到大量的政务数据和敏感信息，如果数据保护不当或存在漏洞，可能会导致数据泄露或被非法获取。这些数据可能包括公民的个人信息、企业的商业秘密以及政府的敏感信息等，

一旦泄露可能会对个人、企业和社会造成严重损失。

为了规避数据泄露风险，数字政府应该采取以下措施：加强数据加密和隐私保护技术的研发和应用，采用先进的加密算法和安全协议，保障数据的机密性和完整性。建立完善的数据访问权限和审批流程，限制对数据的访问权限和操作范围，防止未经授权的人员获取和利用数据。定期进行数据安全检查和风险评估，及时发现和修复数据安全隐患，确保数据的存储、传输和处理过程的安全性。加强与专业的安全机构和厂商的合作，共同推进数据安全技术的研发和应用，提高数据保护的能力和水平。

2. 数据恶意破坏风险

政务数据被恶意篡改、删除或数据平台拒绝服务，可能会造成重大数据资产损失以及政府公共服务失序。这些恶意行为可能是出于政治、经济、社会等目的，对数字政府的建设和运行造成严重的干扰和破坏。

为了规避数据恶意破坏风险，数字政府应该采取以下措施：加强数据的备份和恢复措施，确保数据在遭受攻击或破坏后能够迅速恢复和恢复正常服务。建立完善的安全审计和监控机制，对数据的访问和操作进行记录和监控，及时发现和阻止恶意行为。采用入侵检测和防御技术，加强对外部攻击的监测和防御能力，及时发现和应对网络攻击事件。加强员工的安全意识和技能培训，提高员工对数据保护的重视程度和防范能力。

3. 数据违规使用风险

政务数据共享后，数据使用者可能会误用数据或将数据用于不当用途，从而对数据主体造成不良影响。如政府部门或企业滥用数据、泄露数据或进行不正当竞争等行为，可能会对公民、企业和社会造成不良影响。

为了规避数据违规使用风险，数字政府应该采取以下措施：建立完善的数据使用规范和标准，明确数据的用途和使用范围，防止数据的滥用和不当使用。加强数据的审计和监管力度，对数据的访问和使用进行实时监控和管理，确保数据的合规使用。建立数据的分类管理制度，对不同类型的数据进行分类管理和控制，防止敏感数据的非授权使用。加强与相关机构和企业的合作，共同推进数据的共享和利用的创新发展，提高数据的合规使用和综合利用效率。

4. 个人信息保护不足风险

政务数据中包含大量的个人信息，部分数据面向社会开放前，未经过脱敏、截断、遮挡等处理，导致个人信息泄露。这可能会导致公民的个人隐私受到侵犯，同时也会对数字政府的形象和公信力造成不良影响。

为了规避个人信息保护不足风险，数字政府应该采取以下措施：加强个人信息的保护和管理力度，制定严格的个人信息保护制度和规范，确保个人信息的合法使用和保护。在数据开放前进行充分的安全评估和风险评估，确保数据的开放和使用不会导致个人信息的泄露和滥用。

（二）数据隐私风险及应对策略

1. 数据泄露风险

在数字政府建设过程中，涉及到大量的政务数据和公民个人信息，如果数据保护不当或存在漏洞，可能会导致数据泄露或被非法获取。这些数据泄露可能来自多个方面，如内部人员的不当操作、黑客攻击、第三方合作伙伴的数据泄露等。一旦发生数据泄露，可能会对公民的个人隐私和数字政府的公信力造成严重损害。

为了防范数据泄露风险，数字政府应该采取以下措施：加强数据加密和隐私保护技术的研发和应用，采用先进的加密算法和安全协议，保障数据的机密性和完整性。建立完善的数据访问权限和审批流程，限制对数据的访问权限和操作范围，防止未经授权的人员获取和利用数据。定期进行数据安全检查和风险评估，及时发现和修复数据安全隐患，确保数据的存储、传输和处理过程的安全性。加强与专业的安全机构和厂商的合作，共同推进数据安全技术的研发和应用，提高数据保护的能力和水平。

2. 数据滥用风险

数字政府在采集、存储和使用公民个人信息时，如果缺乏有效的监管和规范，可能会发生数据滥用的情况。例如，政府部门或企业滥用公民个人信息进行非法活动，或者将个人信息用于不当用途等。这种数据滥用行为可能会对公民的合法权益造成损害，同时也会对数字政府的形象和公信力造成不良影响。

为了防范数据滥用风险，数字政府应该采取以下措施：建立完善的数据使用规范和标准，明确数据的用途和使用范围，防止数据的滥用和不当使用。加强对数据使用者的监管和规范，建立健全的数据使用审批流程和监管机制，防止数据滥用行为的发生。建立数据的分类管理制度，对不同类型的数据进行分类管理和控制，防止敏感数据的非授权使用。加强与相关机构和企业的合作，共同推进数据的共享和利用的创新发展，提高数据的合规使用和综合利用效率。

3. 数据不透明风险

数字政府在处理和使用公民个人信息时，如果缺乏透明度和公开性，可能会导致公民对数据的真实性和安全性产生疑虑和不信任。这种不透明风险可能会对数字政府的公信力造成损害，同时也会对公民的参与度和满意度造成不良影响。

为了防范数据不透明风险，数字政府应该采取以下措施：加强数据的公开和透明度，建立健全的数据公开和发布机制，及时公开政务信息和重要数据。加强与公民的沟通和互动，建立健全的公民参与机制和反馈机制，及时回应公民的关切和质疑。建立完善的数据审计和监管机制，加强对数据的审计和监管力度，

确保数据的合规使用和安全性。

（三）技术漏洞风险及应对措施

1. 系统安全漏洞

数字政府系统可能存在未被发现的系统安全漏洞，这些漏洞可能被黑客或恶意攻击者利用，导致数据泄露、系统瘫痪或其他严重后果。这种风险主要来自于系统设计的缺陷、软件代码的错误或配置不当等。为了降低系统安全漏洞风险，数字政府应该采取以下措施：定期进行系统安全漏洞扫描和评估，及时发现和修复潜在的安全漏洞。采用最新的安全补丁和更新，确保系统的安全性能得到持续改进。建立完善的安全监控和报警机制，实时监测系统的安全状态，及时发现和处理安全事件。

2. 应用软件安全漏洞

数字政府所使用的各种应用软件可能存在安全漏洞，如 Web 应用程序、移动应用等。这些漏洞可能导致恶意攻击者利用漏洞进行非法访问、数据窃取或篡改等行为。为了降低应用软件安全漏洞风险，数字政府应该采取以下措施：对应用软件进行定期的安全测试和评估，及时发现和修复潜在的安全漏洞。采用安全的软件开发和测试流程，确保应用软件的质量和安全性。对用户输入进行严格的验证和过滤，防止 SQL 注入、跨站脚本攻击等常见攻击手段。

3. 网络安全漏洞

数字政府的网络基础设施可能存在安全漏洞，如防火墙、入侵检测系统等的配置不当或更新不及时，可能导致网络被攻击者渗透或绕过，进而对系统进行攻击。为了降低网络安全漏洞风险，数字政府应该采取以下措施：定期对网络基础设施进行安全评估和检查，确保网络设备和安全策略的有效性。采用最新的网络安全技术和设备，如下一代防火墙、入侵防御系统等，提高网络的安全防护能力。建立完善的网络安全监控和报警机制，实时监测网络的安全状态，及时发现和处理网络安全事件。

四、网络攻击风险及应对策略

（一）高级可持续威胁攻击（APT 攻击）

这种攻击是一种长期、持续的威胁，攻击者会针对目标进行长期的潜伏和持续的攻击。APT 攻击通常会利用各种先进的攻击手段和技术，如社交工程、恶意软件、漏洞利用等，以渗透和破坏目标系统。数字政府是 APT 攻击的重点目标之一，因为政府机构往往拥有重要的信息和数据，并且 APT 攻击可以长时间地窃取数据或者进行其他恶意操作。

（二）勒索软件攻击

这种攻击是一种利用恶意软件加密目标文件或系统，然后向受害者索要赎金的网络攻击。勒索软件攻击通常会利用各种漏洞或者恶意软件进行传播，并加密受害者的文件或者系统，使其无法使用或者访问。数字政府可能成为勒索软件攻击的目标，因为政府机构的系统和数据非常重要，攻击者可以通过加密文件或者系统来获得赎金。

（三）钓鱼攻击

这种攻击是一种利用虚假网站、邮件、链接等手段诱导用户点击，进而窃取用户个人信息或者破坏目标系统的网络攻击。钓鱼攻击通常会利用伪装成正规网站或者邮件的方式，诱导用户输入个人信息或者下载恶意软件。数字政府可能成为钓鱼攻击的目标之一，因为政府机构拥有大量的个人信息和机密数据，攻击者可以通过钓鱼攻击获取这些信息。

（四）分布式拒绝服务（DDoS）攻击

这种攻击是一种通过发送大量无用的请求或者数据包，使目标系统无法响应正常请求的网络攻击。DDoS 攻击通常会利用大量的计算机或者网络僵尸来发送请求或者数据包，使目标系统过载，无法响应正常请求。数字政府可能成为 DDoS 攻击的目标之一，因为政府机构的网站和服务是公众访问的重要渠道之一，攻击者可以通过 DDoS 攻击使网站或者服务无法访问，影响公众的正常生活和工作。

为了应对以上这些网络攻击风险，数字政府需要采取一系列的安全措施，如加强网络安全管理、建立安全审计机制、使用防火墙、入侵检测和防御系统等安全设备来保护系统和数据的安全性。此外，数字政府还需要加强与安全厂商的合作，及时获取最新的安全信息和漏洞修复方案，以应对不断变化的网络威胁环境。

结束语

综上所述，数字政府建设是现代社会治理的重要方向，建设数字政府不仅需要具备核心能力，还面临着多重风险和挑战，需要我们采取有效的措施来规避和管理。通过加强信息安全管理、数据隐私保护、技术漏洞管理和网络攻击防御等措施，我们可以有效地降低数字政府建设面临的风险和挑战。同时，我们还需要不断适应新技术的发展和经济的需求，加强数字化服务的能力和水平，为数字政府的建设和发展做出更大的贡献。

参考文献：

[1] 赵娟，孟天广 . 数字政府的纵向治理逻辑：分层体系与协同治理 [J]. 学海 .2021,(2).

[2] 王谦，曾瑞雪 . 社会技术系统框架下”数字政府”风险分析及治理 [J]. 西南民族大学学报（人文社科版）.2020,(5).

[3] 张成福，谢侃侃 . 数字化时代的政府转型与数字政府 [J]. 行政论坛 .2020,27(6).34-41.

作者简介：董倩（1984.07—），女，满族，辽宁抚顺人，大学本科学历，工程师。研究方向为“数字政府”建设及经济社会发展。