ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.11, No.2, January 2015
E-mail: wyl@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964

# 我国“互联网+政务”系统安全体系研究

许翔燕

（成都信息工程大学，四川 成都 610103）

**摘要：**“互联网+政务”是新一代信息技术手段，是国家实施政府组织机构职能转变，工作流程优化重组，提高政府管理、公共服务和应急能力的重要措施，有利于带动整个国民经济和社会信息化的发展。政务数据涉及国家基础数据、宏观经济数据和地理信息数据等国家核心机密及很多各个行业的重要数据，直接关系到一个国家的政治、军事、经济等领域的安全和稳定。新的技术带来新的安全隐患。构建安全管理保障体系能让互联网+政务系统保持畅通，提高政府政务能力，提高政府公信力。

**关键词：**互联网+；信息安全；云计算；大数据；架构

**中图分类号：TP311　　文献标识码：A　　文章编号：1009-3044(2015)02-0266-03**

DOI:10.14004/j.cnki.ckt.2015.0924

**"Internet + government affairs" System Security Architectural Study in China**

XU Xiang-yan

(Chengdu University of Information Technology, Chengdu 610103, China)

**Abstract:**"Internet + government affairs" is a new generation of information technology, is the national implementation of the government function change in your organization, workflow optimization restructuring, improve the government management, public service and emergency ability of the important measures, to promote the development of the whole national economy and social informatization.E-government data involving state data, macroeconomic data and geographic information data such as core state secrets and a lot of important data in a wide range of industries, is directly related to a country's political, military, economic and other fields of safety and stability.New technology brings new security hidden danger.Building security management security system can keep Internet + e-government system, improve the government administrative ability, improve the government's credibility.

**Key words:** Internet +; information security; cloud computing; big data; architecture

## 1 引言

随着移动互联网、大数据、云计算等新一代信息技术的迅猛发展，大力推动各个行业的信息化发展，“互联网+政务”因运而生。我国政府决策者制定很多政策大力推动运用大数据、云计算、“互联网＋”等技术实现创新。我国电子政务水平也将随着“互联网+”行动计划的实施不断提高。智慧的政务恰恰是建立在以服务为导向的电子政务系统。

“互联网+政务”的底层平台是云平台，而云平台的基础平台是互联网。而目前使用的互联网在当初设计的时候基本没有考虑安全，自身缺少设防和安全隐患多。互联网犯罪属于新兴犯罪，很多国家缺乏相应的法律法规，而且各个国家的标准不一致，网络无国界，大量的跨国网络犯罪给执法也带来很大的难度。甚至国家与国家之间利用互联网截取对方国家机密，使基于互联网开展的电子政务应用面临着严峻的挑战。在信息技术广泛应用于各个领域的条件下，信息安全在国家安全中占居战略地位。

## 2 “互联网+政务”系统概述

### 2.1 “互联网+政务”系统架构

“互联网+政务”主要提供三种服务：公众服务（公众服务外网）、内部核心业务（业务内网）、和数据交换层（政务专用网）。业务内网是一个完整的政务内部办公环境，公众服务外网担负着政务服务与公众间信息沟通的任务，而政务专用网则负责各级政府职能部门内部与部门之间的数据交换。“互联网+政务”系统架构如图1所示：


**图1 “互联网+政务”系统架构**

收稿日期：2014-12-06

作者简介：许翔燕（1978—），男，四川仪陇人，成都信息工程大学讲师，硕士，主要研究方向：数据挖掘，计算机网络等。

云平台是“互联网+政务”整个体系的基础,以互联网、移动互联网为支撑,包括分布式处理平台及云存储平台。云平台在技术路线设计上充分考虑扩展能力,做到灵活、安全、高效、可靠。主要提供计算和存储服务满足政务系统的实际需求。数据处理层主要提供各个业务部门需要的数据,能对大数据进行分析功能。业务应用层主要是政务部门业务进行分析,处理,为具体业务应用提供支持。消息层主要与用户沟通,搜集用户需求,按需分配数据。安全管理体系通过制度、技术的支撑,各个系统之间的融合联动进行主动防御,第一时间消除安全隐患。为政务网建设全面的智能安全保障。运行与维护体系集资源、业务与用户(接入用户的安全准入与审计)三者的管理于一体,模块化的结构使用户可以“按需构建”管理系统,在网络与业务间智能关联,为政务外部平台提供架构统一,保障系统的畅通运行。

### 2.2 “互联网+政务”系统安全问题

目前我国“互联网+政务”中的安全问题主要表现在:

#### 2.2.1 管理制度不健全

我国政务安全管理制度工作比较滞后。由于很多新生事物的出现,配套的管理制度没有跟上,在很多方面还出现法律制度的真空地带。如在信息泄密的判定、信息传播的责任划分等方面都还有很多不健全的地方。我国部分政务工作者认为只有专业人士才能很好的使用,人为扩大了信息技术提供者和使用者之间的“数字鸿沟”,加大了信息安全的隐患。很多部门没有从管理制度、技术和人员上建立相应的安全防范机制,缺乏行之有效的安全检查保护措施。

#### 2.2.2 缺乏安全意识

受传统政务办公的影响,我国很多政务系统管理和操作人员对新信息技术还未接触或接触不多,对高新信息技术应用方面的能力也比较欠缺,管理人员违规或违法操作、不少技术维护使用人员不遵守安全保密规定,将内网、专网直接或间接地与外网连接,管理人员的整体素质还有待提高,有的安全设备配置不合理,访问控制不够严格,这些问题的存在直接带来严重的安全问题。

#### 2.2.3 业务相互独立、分散异构

我国政务系统业务相互独立,各自建立自己的系统,缺乏统一身份认证,没有统一的数据基础库,业务的敏感性和业务系统之间的相互操作较少,业务数据的安全、业务系统之间的相互责任等安全问题成为政务建设中必需要解决的重要问题。虚拟化终端使用过程中,由于账户成为了控制资源是否允许使用的唯一控制方式,通过身份冒用可以越权使用非授权信息,造成涉密信息的泄密。采用虚拟化技术的云终端,数据统一存储在核心存储设备上,数据集中存储后,敏感数据均存储在服务器上(云端),存在非授权使用和非法访问等安全隐患。

#### 2.2.4 系统设计不合理

部分政务系统完全依托第三方开发公司,自身很少参与系统设计,而开发公司对业务流程不太熟悉,不知道哪些数据重要需要加密或保密,在系统本身设计开发过程中缺乏安全管理体系,更有甚者系统本身就存在安全漏洞。

#### 2.2.5 病毒破坏、黑客攻击

计算机病毒会造成系统破坏,数据破坏,网络堵塞。黑客入侵、信息间谍、敌对势力、恐怖集团、国家之间信息战攻击。采用非法侵入国家重要信息系统,偷窃、篡改或破坏系统功能或数据等手段,造成系统瘫痪,给国家造成重大政治影响和经济损失。互联网上针对政务系统的违法犯罪活动日益增多。

## 3 “互联网+政务”安全体系

业务的错综复杂,各种各样的运行环境,给系统带来了大量潜在的安全隐患:网络本身的安全问题、软件系统的漏洞不可避免、数据在传输过程中的丢失及泄露、管理疏忽、伪造身份进入系统、黑客的恶意攻击、病毒入侵等等。这些安全隐患不可能完全依靠安全技术得到解决,必须结合政务整体安全需求的基础上构建安全管理保障体系。

| | |
|---|---|
| 安全管理保障体系 | 响应与恢复机制(云存储、数据备份与恢复) |
| | 预警检测体系 |
| | 安全技术支撑平台(操作系统、数据库、信息管理系统、网络) |
| | 基础安全服务设施(网络域、网络隔离) |

图2 “互联网+政务”安全体系

“互联网+政务”安全体系如图2所示,主要由五部分组成:安全管理保障体系、基础安全服务设施、安全技术支撑平台、预警检测体系、响应与恢复机制。安全管理保障体系是整个安全体系结构的灵魂。

### 3.1 安全管理保障体系

安全管理保障体系是整个体系中的灵魂,从政务系统的设计到运行维护,都需要法律法规、制度的支撑。我国政务安全涉及到法律、管理、技术等多方面的原因。在安全体系中,管理占有相当大的比重,任何完善的安全技术如果没有完善的管理制度做保障都没有安全可言,所以建立定期的人员培训管理、策略管理、安全检测、数据备份管理、日志管理等一系列管理方法和制度是非常必要的。信息实行分级管理与维护。信息必须审计查看,从用户行为分析、信用度体系等各个维度识别恶意消息。实行敏感信息过滤、垃圾信息检查机制。

### 3.2 基础安全服务设施

基础安全服务设施网络是整个体系结构中的基础,安全必须构筑在一个坚实的安全服务基础之上,支撑整个政务安全稳定的基础是信任。基础安全服务设施的作用就是为政务系统建立一个可相互信任的云环境,为其他安全技术的实施提供正确决策的基础。这其中必须解决的问题包括:

#### 3.2.1 硬件保障

主要涉及分布式服务器、网络设备、终端及存储设备等核心IT基础设施的安全。

#### 3.2.2 网络保障

政务应用中势必存在内部与专用、外部服务间的信息交换需求,虽然一切数据都存在云端,然而基于内部数据保密性的考虑,就势必解决私有云与公有云之间数据的交换安全。云之间的访问必须有严格的审计控制、网络域的控制,只有经过认证的设备可以访问网络,并且能明确地限定其访问范围。在业务之间采取访问隔离策略,防止应用间内部恶意访问的安全问题。可以利用第三方的认证系统加强认证的安全强度,如证书(CA)等系统。使得电子政务网络处于中心可管理的状态,从而使得各种网络域管理策略得以实现。从而准确了解和控制

访问设备的访问位置及访问权限。

#### 3.2.3 标准时间源

对于政务公务执行审批的应用来说，系统中的文件都应该具有可信的时间戳。政务公文上的时间标记是重要的政策执行依据和凭证，建立可信统一的时间源可以通过在标准时间源上附加数字签名的方法来防止时间在传输途中被篡改情况的发生。

#### 3.2.4 统一身份验证

政务系统会根据用户的身份决定是否执行其提出的访问要求，用户身份是否可信就成为了该安全策略的核心问题。政务系统用户可以统一使用身份证号码或个人标识，学习国外发达国家每个人拥有唯一身份标识，使用固定密码+动态密码方式进行密码校验，有效保证密码安全。身份认证和访问管理包括：认证、授权和用户配置文件管理，以及能满足各种用户和访问流程自动化需求的开放式应用程序接口等。

#### 3.2.5 数据安全

通过认证的用户从系统中获得的数据应该被相信是完整未被篡改的，同时数据在传输过程中应该是安全机密不可破解的。不同应用之间的数据是隔离的。所有数据在操作过程中应做到事前扫描和事后审计。

### 3.3 安全技术支撑平台

#### 3.3.1 云平台搭建及维护技术

Hadoop、spark平台搭建及维护技术；掌握云计算机的基础架构即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS）。

#### 3.3.2 操作系统维护技术

政务应用和安全措施(包括防火墙、防病毒、入侵检测等)都依赖操作系统提供底层支持。操作系统的漏洞或配置不当将有可能导致整个安全体系的崩溃。在操作系统、服务器软件配置上进行了加固，防止系统级别的安全漏洞，并会及时周知开发者进行相应的处理。政务系统还包括各种终端的应用。主要使用操作系统：Windows系列、Unix系列、Linux系列。

#### 3.3.3 网络管理及维护技术

政务系统涉及到职能部门之间、上下级之间、区域间的公文流转，公文的信息往往涉及到机密等级的问题。在信息传递过程中，必须依赖互联网。必须掌握基本的IPV4或IPV6协议、网络防火墙、IPsec加密技术、Vlan、VPN、客户端绑定MAC地址或IP技术、端口隔离等网络基本操作技术。

#### 3.3.4 数据库管理及维护技术

主要掌握云数据库、oracle、SQL server、mysql等数据库操作及加密技术；学习大数据技术，能对大数据进行分析处理。

#### 3.3.5 政务软件系统开发、管理及维护技术

当前主流的.NET及Java开发技术，能灵活利用软件工程来进行管理和维护政务系统。

### 3.4 预警检测体系

多层次、多维度的实时监控和离线分析 。预警检测体系包括入侵检测、漏洞检测、接入检测等。可以了解系统的运行状况和发生的安全事件，并根据检测情况来提前预防和调整安全策略。

### 3.5 数据备份与容灾恢复机制

政务数据涉及国家基础数据、宏观经济数据和地理信息数据等国家核心机密及很多各个行业的重要数据。硬件故障、自然灾害、网络攻击、病毒破坏等都有可能导致政府重要数据的丢失，必须建立一套响应与及时恢复机制。

云平台在数据备份方面已具有其本身的优势，但根据政务系统其特点，应该具备以下条件：

1）云存储支持异地备份与恢复；

2）支持多种存储介质和备份模式；

3)支持自动恢复机制。

## 4 结论

“互联网+政务”肯定会给电子政务带来创新，提高政务办事效能，电子政务安全不能仅仅依靠信息技术，而应该构建一个安全体系，才能保障电子政务的正常运营，防患于未然。

## 参考文献:

[1] 邬贺铨. 电子政务安全体系[J]. 信息安全与通信保密，2003(4).

[2] 刘杰彦,眭建军. 电子政务中基于SAML的信任与授权服务系统设计[J]. 计算机应用研究，2007,24(7).-111-113,150.

[3] 褚俊,苏震. 电子政务安全技术保障[M]. 北京中国人民大学出版社，2004.

[4] 张薇. 从互联网环境看中国电子政务安全挑战[J]. 电子政务，2012(5).

[5] 黎水林. 我国电子政务安全体系结构研究[J]. 管理研究，2010(5).

[6] 秦天保. 电子政务信息安全体系结构研究[J]. 计算机系统应用，2006(1).

[7] 张振,王惠芳. 电子政务安全体系结构研究与设计[J]. 网络安全技术与应用，2010(6).

[8] 王谦, 陈放. 我国电子政务信息安全及保障体系[J]，网络安全技术与应用，2006(4).

[9] 吕元智. 基于云计算的电子政务信息资源共享系统建设研究[J]. 情报理论与实践，2010(5).

[10] 张彦超, 赵爽. 基于云计算的电子政务公共平台:安全风险与应对策略[J]. 电信网技术，2014(2).

[11] 尹洁. 凉山州电子政务建设中的安全集成[J]. 西昌学院学报：自然科学版,2009(9).