在新形势下构建我省电子政务网络安全保障体系

广东省经济和信息化委员会

电子政务处（信息安全协调处）姜宝

CONTENTS

目录

01 我们所处的形势分析

02 国家和省的战略部署

03 电子政务网络安全现状及问题

04 展望

分析网络安全必须先分析信息化。习近平总书记指出“**安全是发展的前提，发展是安全的保障，安全和发展要同步推进。**”这个著名的论断辩证而统一，非常形象的概述了网络安全与信息化的关系。

（一）我们身处于何处？

我们身处一个伟大的时代。简言之是互联网时代，一个基于大数据、云计算和人工智能的时代。

手机等终端，已经成功将我们连入了整个世界，互联网世界。这便是我们身处的时代，**连接**一切的时代。

（二）这个时代的基本特征

变化

变化是必然的，一切都在变化之中，我们生活中每一项显著变化的核心都是某种科技，某种算法。带动现代社会变化的核心，是信息化。不断的变化意味着流程比产品更加重要。流程不仅指业务流程，更多的是创造出科技产品的科学方法。“小步快跑，快速迭代”的腾讯理念，就是对变化的最好响应。

那么问题来了，我们网络安全如何去适应这种变化？

（二）这个时代的基本特征

流动

信息混杂的上万亿条数据汇聚一起，相互流动，便是我们通常所说的“云”。流动，导致了互联网充斥着大量的复制品，一个热点，一秒之内会被复制几百万次，不同的客户端都会同时提醒你去看。那什么是无法复制的呢？信任，信任是虚拟网络时间的基础，它无法生产，无法复制，亦无法购买。信任的背后是什么呢？安全。在不安全的网络环境下，信任会被破坏。比如说：网络刷票，淘宝刷钻，赚好评，本质上都是安全的问题。

（二）这个时代的基本特征

智能

去年以来，代表着这个世界上最强的十几位最强大脑，在围棋领域完败。阿法狗的背后，是分布式、网络、大数据支撑、云计算，以及最为核心的人工智能计算。这种基于云端和大数据的人工智能计算拥有“改变一切”的力量，而且便于复制，能推广到我们任何的行业和领域，比“互联网+”更为的聪明而有效。同理，我们网络安全领域可否拥有一条阿法狗？比世界上顶级的黑客还要厉害？

（三）我们担负的使命？

互联网的蓬勃发展，带来了网络安全问题，各种各样的网络安全事件层出不穷，大家都是行家，我不一一列举，我想问的是为什么近年来，可以持续成为全国“两会”的热点议题？从本质上来分析，**互联网已经关系到人民群众的切身利益**，网络安全，无人可以置身事外。

涉及所有人切身利益的事情概况起来主要有衣、食、住、行、教育、医疗。如今又多了一个网络。当每个人都关心一个事情的时候，这个事情的重要性和优先级就会发生变化。

CONTENTS

目录

01 我们所处的形势分析

02 国家和省的战略部署

03 电子政务网络安全现状及问题

04 展望

（一）国家的网络强国战略

为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展。

党中央国务院从战略的角度成立了以习近平总书记为组长的中央网络安全和信息化领导小组，首次提出“**网络强国**”战略，习总书记对网络安全的系列讲话值得我们每一位网络安全人细细研读，可以说是已经涵盖网络安全的各个方面。从事网络安全工作的企业，更加要深入细致的学习，这里面有未来网络安全发展的方向。

（二）国家网络安全法

为网络安全立法工作十年磨一剑，《中华人民共和国网络安全法》于2016年正式出台，为我们今后的网络安全工作指明了方向，为依法治网提供了法治保障。这是一个划时代的法律，我个人认为一个行业只有拥有属于自己的法律，才能算的上真正意义的行业，网络安全作为比信息化晚出现的事物，能早于信息化立法，可以说是一个巨大的进步。

国家明确指出“对公共通信和信息服务、能源、交通、水利、金融、公共服务、**电子政务**等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。”

（三）《广东省信息化促进条例》

1 网络安全总体性的规定

第六章 信息安全保障和监管

第五十七条 县级以上人民政府应当建立信息安全工作领导协调机制，统筹协调和指导本行政区域内的信息安全保障和监管工作。**县级以上人民政府信息安全协调保障主管部门**应当会同公安、国家安全、保密、密码管理、广电、通信管理等部门，建立和完善信息安全保障协调机制，完善信息安全保障体系，协调和指导重要信息网络和信息系统容灾备份建设，加强信息安全管理和能力建设。

2 政府加强信息安全监管

第五十八条 各级人民政府应当加强信息安全监管，及时建立大数据、云计算、物联网等新技术新产品在政府及其他重点领域应用的标准、规范，建立和完善风险评估和监测、检查、管理体系，及时预警信息安全隐患，保障网络、信息系统、信息资源资产的安全。

3 信息安全保障工作责任制

第五十九条 信息网络和信息系统的所有者或者运营者应当依据国家有关规定以及相关技术标准，建立信息安全保障工作责任制，制定本单位信息安全保护和容灾备份措施，对信息网络和信息系统实行信息安全等级保护，定期进行信息安全风险评估。

4 电子签名

第六十一条 县级以上人民政府信息化主管部门应当会同有关部门，在电子政务、电子商务、公共服务等领域推广使用电子签名，鼓励电子签名认证数字证书在互联网上的应用；推动与港澳台电子签名认证证书的互认互通。

信息化主管部门、密码管理部门应当按照国家有关规定，对电子认证服务机构和电子认证服务实施监督管理。

5 信息安全应急处置协调与通报

第六十二条 县级以上人民政府信息化主管部门应当会同有关部门，建立和完善信息安全应急处理协调机制和信息安全通报制度。

信息网络和信息系统的运行、使用单位，应当制定本单位信息安全应急预案，定期开展应急演练，增强信息网络和信息系统的抗毁能力、灾后恢复能力。

发生重大信息网络与信息系统安全事故后，相关单位应当迅速采取应急措施降低损害程度，防止事故扩大，保存相关记录，并按照规定向有关部门报告。

（四）《广东省电子政务发展规划（2014-2020）》

这个规划是由省经信委牵头草拟，省政府印发的，指导我省电子政务工作的一份纲领性的规划。他不仅提出了要对电子政务网络、云平台、数据资源共享交换进行集约化建设，还对网络信息安全工作，提出了明确具体的任务。

1 完善电子政务信息安全协调机制

建立健全省、市、县电子政务三级网络与信息安全协调工作机制，统筹协调指导全省电子政务信息安全保障和监管工作，落实电子政务信息安全责任制。建设完善广东省电子政务信息安全联合工作平台，上联国家、下联市县、横联各级政府部门，及时发布信息安全评估、监测、预警信息，提高政府部门信息安全联动响应能力。

2 提升电子政务信息安全管理水平

加强电子政务网络和互联网出口的统筹管理。做强内网，提高政务内网涉密信息的保密水平；做大外网，实现政务外网对政府非涉密业务的全覆盖；建设电子政务外网互联网出口汇聚平台。加强电子政务信息资源、应用系统生命周期安全管理。建立电子政务供应链安全管理体系，在政府采购、建设、防护、运维等环节中实施信息安全审查和评估，提高政府信息化资产安全管理水平，逐步提高安全自主可控的国产软硬件产品在政府信息化资产中所占的比重。

3 构建电子政务信息安全服务支撑体系

实施电子政务信息安全保障支撑计划，加强电子政务监测评估预警，建设省、市、县三级电子政务务外网和互联网实时监测体系，对电子政务信息系统进行在线实时风险评估，重点围绕省网上办事大厅、社会治理等重要政务应用开展风险预警服务。建立电子政务软件质量和集成水平评估体系，加强对政府信息化资产上线前的测评和检查，提高电子政务应用系统软件质量和集成水平。

3 构建电子政务信息安全服务支撑体系

建设省数字证书交叉认证体系，实现数字证书“一证多用、多证互通”，提高政府服务的安全性和便利性。建立广东省政府部门可使用IT企业产品目录，提升自主可控的信息产品覆盖率，带动我省安全可控信息产业发展。

（五）《广东省电子政务网络信息安全预警通报反馈暂行管理办法》

第一章 总则

第一条 为建立健全广东省电子政务网络信息安全预警通报反馈工作机制，规范电子政务网络信息安全预警管理，推动党政机关及时高效地发现、处置网络信息安全预警信息，预防和减少网络信息安全事件造成的损失和危害，结合本省实际情况，制定本办法。

第二条 本办法适用于广东省电子政务网络信息安全预警信息的通报反馈工作。

第三条 电子政务网络信息安全预警通报反馈工作遵循“快速反应、科学处置、及时反馈、闭环管理、信息保密”原则。

CONTENTS

目录

01 我们所处的形势分析

02 国家和省的战略部署

03 电子政务网络安全现状及问题

04 展望

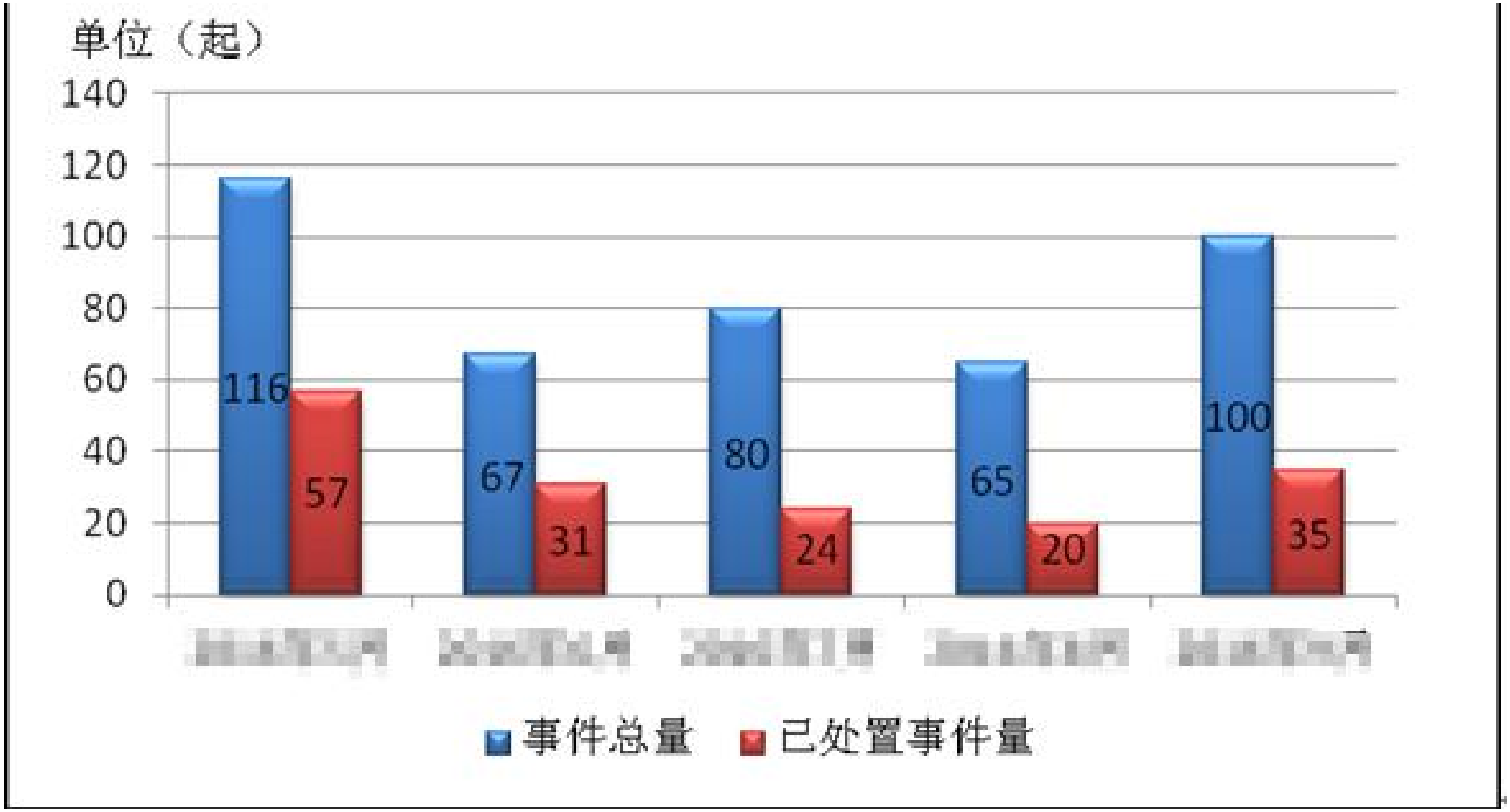
我省近年来积极贯彻落实国家和省的决策部署，严格按照网络安全与信息化“同步规划、同步设计、同步建设”，要求所有政府部门信息化项目在规划之初，就预留网络安全资金，在设计之初，要有网络安全预算，在建设之时，要使用网络安全产品和服务。没有做到以上几点项目，我们会退回整改。

我们建成省级电子政务网络信息安全保障服务体系。构建上联中央、下联市、县的联动协调机制，建立高效顺畅的四级电子政务网络安全预警通报反馈机制和形成网络安全事件“预警发布、跟踪支撑、处置反馈”的闭环工作机制。目前已经做到网络安全事件高效处置，以近期的Struts2漏洞为例，从国家下发预警，到我们通知到具体市、县负责的同志，总共只花了几个小时，就完成几百个具体政府网站的预警。

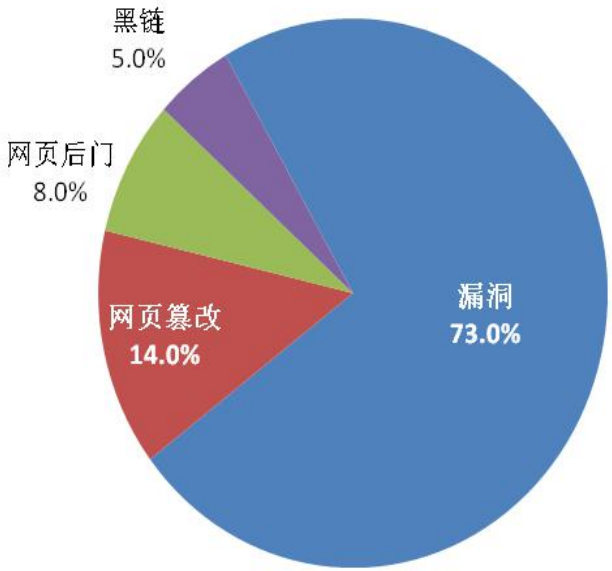
总体而言，我省电子政务网络安全状况是良好的。全省电子政务网络运行总体平稳，电子政务外网各项监测指标正常，未发生较大以上网络安全事件。

但是问题依然非常突出，主要表现在：

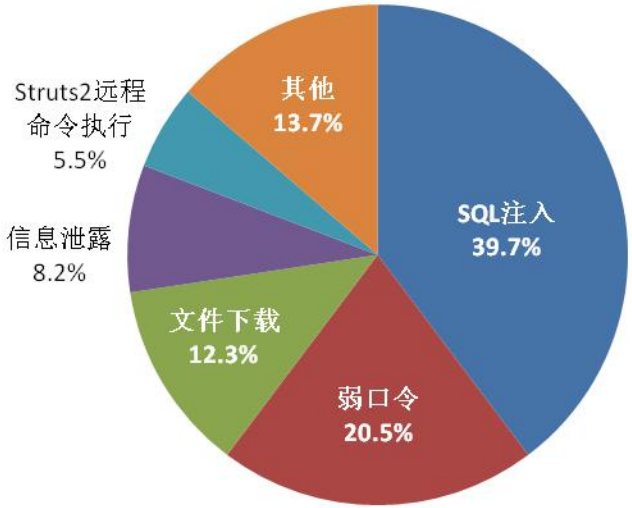
（一）电子政务网络信息安全事件整改不及时



从类型上分析，我省电子政务安全事件漏洞类事件73起（占73.0%），网页篡改事件14起（占14.0%），网站后门事件8起（占8.0%），网站暗链事件5起（占5.0%）。

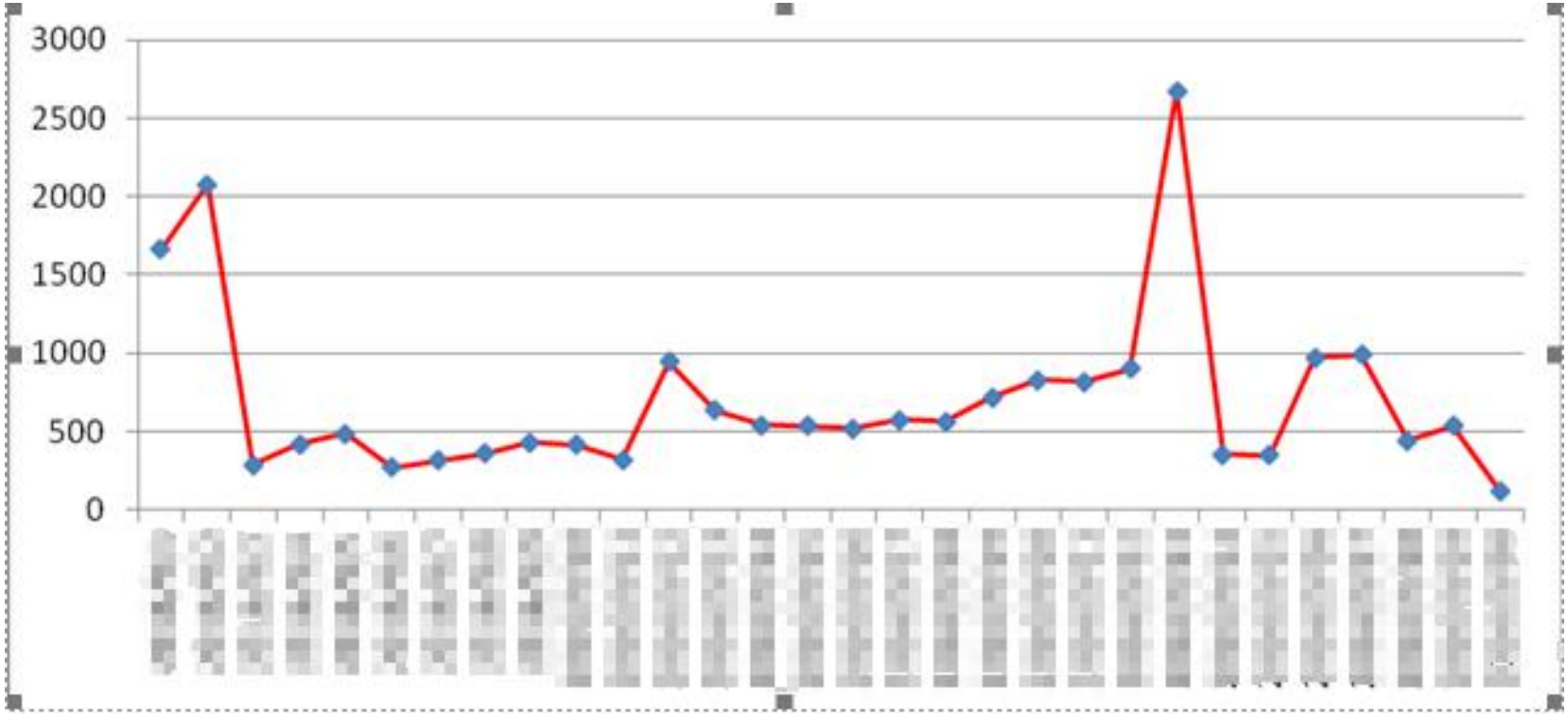


进一步分析网站漏洞类事件的类型分布情况如图所示，SQL注入事件（占39.7%）居首位，其次是弱口令漏洞（占20.5%）。上述两类漏洞占比之和超过全部事件的60%。



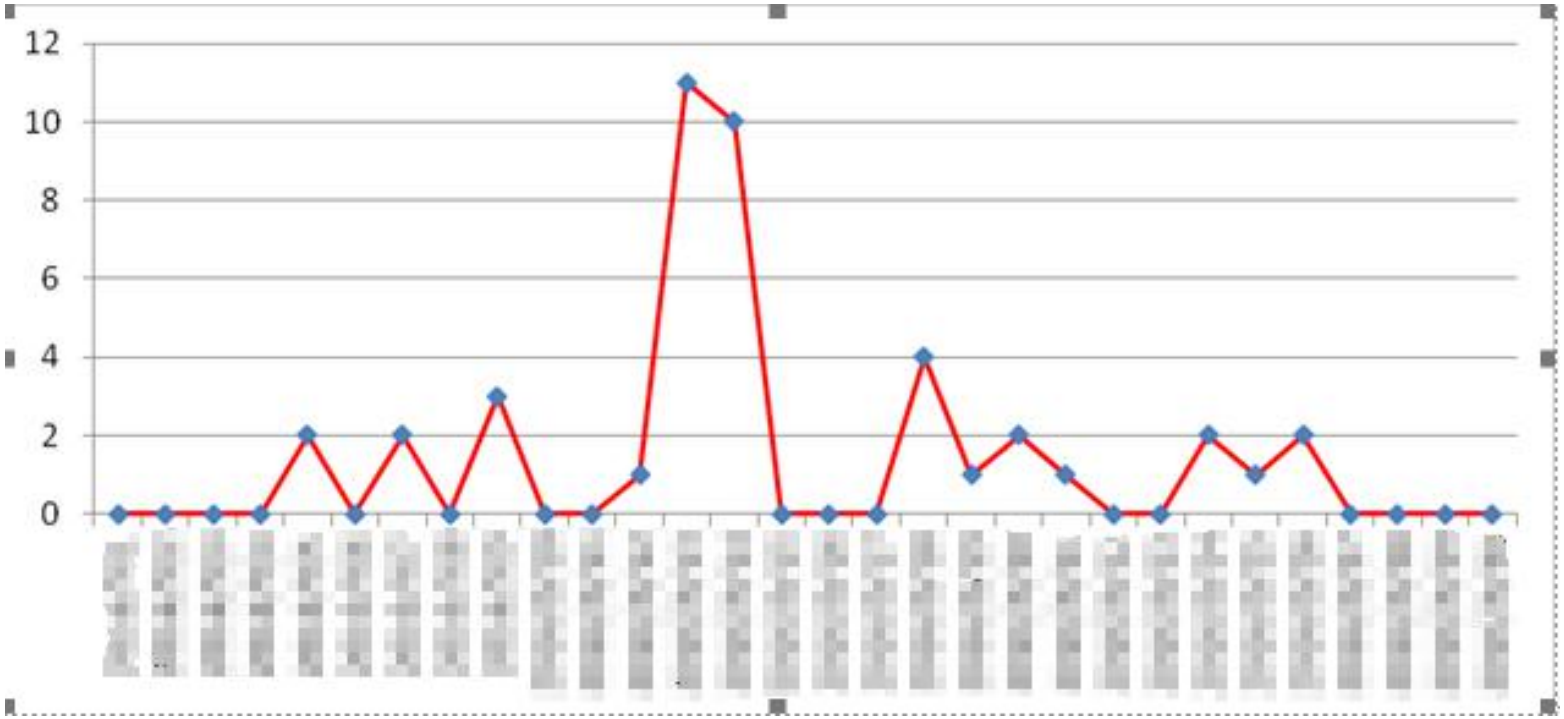
（二）频繁遭受互联网攻击

以2016年某月为例，来源于互联网的尝试攻击21,030次，日均约为701次，较上月日均次数增加16.3%，单日尝试攻击次数最高达2,675次。



（二）频繁遭受互联网攻击

恶意代码疑似感染事件42起，恶意代码感染事件每日发生次数变化趋势如下图所示，其中，最大值达到11次/日。



CONTENTS

目录

01 我们所处的形势分析

02 国家和省的战略部署

03 电子政务网络安全现状及问题

04 展望

（一）加强电子政务网络信息监测预警体系建设

应进一步加强电子政务网络信息监测预警体系建设。更加灵敏的感知网络安全态势。应在互联网出口、电子政务网络平台互联网域等关键节点部署基于大数据、云计算的网络安全产品。

（二）大数据安全感知，多方共享网络安全信息

中央、省、市、县共享共有网络安全信息，开展大数据安全感知，研究网络安全事件规律，提早预判和防范网络安全攻击。

（三）完善数字证书交叉认证平台建设

完善数字证书交叉认证平台建设，实现国内ca间的互认，构建基于数字证书的网络信任基础体系。建设基于移动端的证书服务功能；推进粤港、粤澳电子签名互认工作。

谢　谢