学校编码：10384　　分类号_____密级_____
学号：X2010230677　　UDC _____

厦门大学

工 程 硕 士 学 位 论 文

税务部门信息安全体系设计与实现

Design and Implementation of Information Security System Building for Tax Department

王晨

指 导 教 师： 王 备 战 教 授
专 业 名 称： 软 件 工 程
论文提交日期： 2012 年 10 月
论文答辩日期： 2012 年 11 月
学位授予日期： 2012 年 月

答辩委员会主席：_____
评 阅 人：_____

2012 年 11 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

信息革命是人类历史上继农业革命、工业革命之后，又一个伟大的变革。它已经对人类的生活方式、工作方式乃至整个社会的结构产生了深远的影响，人类工作和生活已经离不开信息技术。税务部门信息系统是涉及国家安全、经济命脉、社会稳定的基础信息网络和重要信息系统。它的安全、稳定、可靠地运行，不仅与国内各个行业密切相关，甚至影响着人们的日常生活。

税务部门信息安全体系是一个多层次、多因素、动态的过程，要求综合思考和统一规划。同时还要注意监控系统内外环境的变化，很可能某一环节上的安全缺陷就会对整个信息安全体系构成威胁。

论文首先介绍了国外税务部门信息化现状和世界主流的信息安全标准框架，描述了我国税务部门信息化和信息安全发展历程，阐述我国税务部门信息化发展的特点。

其次，通过现场评估工作得出税务部门面临的威胁、安全现状和安全需求。其中，安全现状包括技术现状、管理现状和人员现状。安全需求包括技术安全需求、管理安全需求和人员需求。

然后，通过使用模型来进行信息安全体系建设的设计。同时，严格按照设计方法、流程和原则，总体设计和分步实施。

依次，按照面临的威胁、安全现状和安全需求，综合税务部门有关要求和同类行业成功经验，进行信息安全体系设计，依据信息安全平台设计原则，提出了以业务连续性为目标，安全管理、安全技术为支柱，信息和信息系统为保护对象，安全策略为手段，信息安全平台为核心的整体的信息安全体系。

最后，介绍了信息安全体系的核心信息安全平台的实施过程。

关键词：信息安全；体系建设；安全平台

Abstract

Information revolution is another great transformation after agricultural revolution and industrial revolution. It already has been exert profound impact on life and work style of humankind, even on the entire social structure. Information system of tax authorities is related to national security, economic lifeline and social stability. Its running has great influence on various sectors and people's daily life.

Information security system of tax authorities is multi-level, multi –factor and dynamic. It requires synthetic thinking and unified planning. The changes of internal and external environment should be monitored in the meantime because even a minor security flaw could pose great threat to the all information security system.

Firstly, the dissertation introduces the current situation of information of tax authorities and mainstream standard framework of information security both home and aboard. It reviews the development of information and information security of tax security in our country and expounds on the characteristics of information development.

Secondly, security threat, security status and security requirements are obtained through on-site evaluation. Security status entails technical status, management status and personnel status. Security requirements involve technical security requirements, management security requirements and personnel requirements.

Thirdly, it focused on the designing of information security system with the help of models and overall design and step-by-step implementation is conducted strictly based on by design method, process and principle.

And then, the design of information security system in conducted based on threat, security status, security needs and requirements of related tax departments. The information security system is set up in accordance with design principle of information security platform. The goal of information security system is business continuity and the core of information security system is information security platform.

Lastly, it concludes with the implement process of information security platform.

Key words: Information Security； System Construction； Security Platform

目录

Contents

第一章 绪论

1.1 研究背景

信息革命是又一个伟大的革命。在人类进入 21 世纪迈进信息社会之后，由于计算机、通信和网络等科学技术迅猛发展，凸显了信息要素对于个人对于社会的重要性。人类社会从物质和能源过渡到物质、能源和信息三位一体的新时代，信息与物质和能源一起构成社会发展的三大原动力。随着信息革命的到来，个人的生存和发展变得与获取外部信息的数量和质量密切相关。为了适应社会和改造社会，必须及时、充分、准确的获取和处理大量的信息。[1]

当信息成为社会发展的基石之后，围绕信息的争夺愈演愈烈。特别是在信息技术高速发展的今天，我们把大量有价值的信息保存在计算机和网络中，这已经成为黑客、间谍等不法分子的攻击目标。许多不法分子为了获得有价值的信息发动的攻击次数逐渐增多，这严重阻挠了世界各国正常的政治、经济、文化等活动。当信息安全事件数量不断增多，危害性不断增大，造成的后果越来越严重，信息安全随之上升到国家战略，成为国家安全和社会稳定的关键点之一。

例如：英国曼彻斯特议会 IT 系统于 2009 年 2 月因感染“飞客”蠕虫病毒而中断，造成约 150 万英镑的损失。[2]黑客组织“匿名者”在互联网上发布声明，计划于 2012 年 5 月 25 日对全球 46 家企业（包含中国石化、中国石油、国家电网、中国银行和东风汽车 5 家中国企业）发起分布式拒绝服务攻击。[3]

图 1.1 为中国互联网应急中心接收非扫描类事件年度统计图（2003 年-2011 年）。

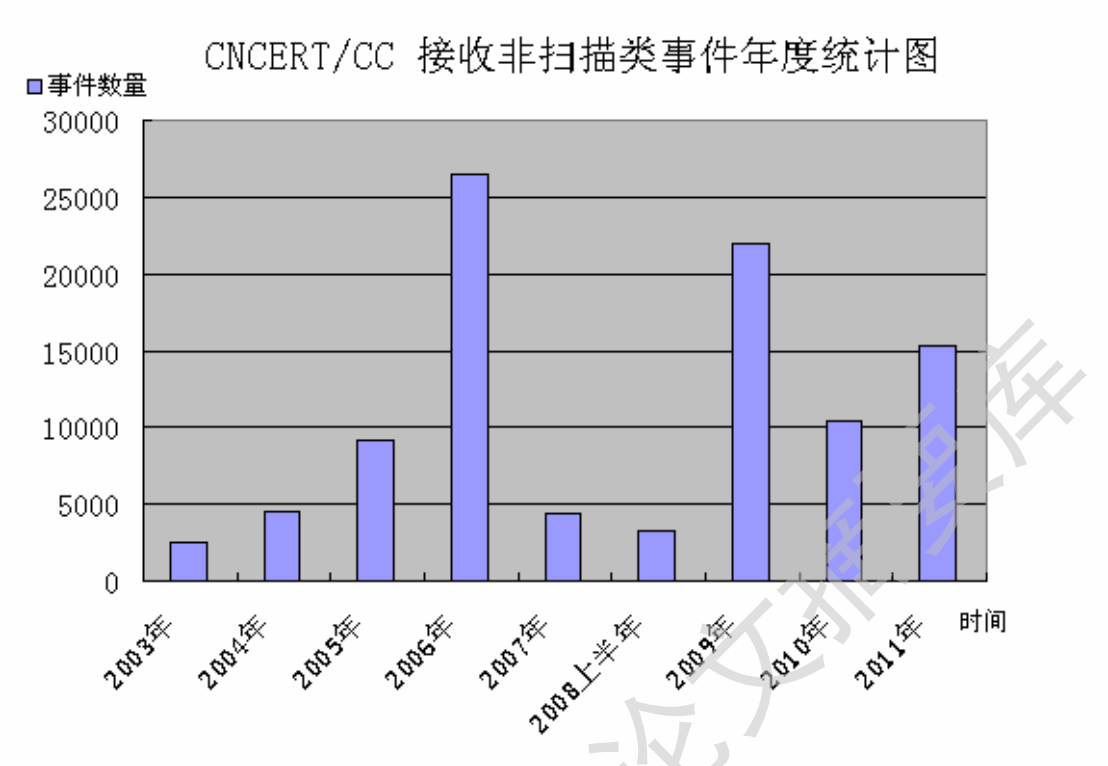

图 1.1 CNCERT/CC 接收非扫描类事件年度统计图（2003 年-2011 年）

数据来源：中国国家互联网应急中心、《互联网安全危险报告（年报）》、 2003 年到 2011 年. [4]

当前，税务部门信息系统和网络规模不断扩大，互联网业务不断增多，各种应用系统不断完善，与其他部门的横向连接也日益紧密，随之而来的源自内部和外部的各种安全威胁也越来越显著，由此对税务部门信息安全建设提出了新的要求。当各种不同的安全技术手段部署使用后，人们认识到信息安全不仅仅只是技术问题，而且包括法律法规、管理制度、人员意识等各方面因素，是一个体系。

1.2 国内外现状

1.2.1 各国现状

信息技术给人们的生产和生活方式带来了巨大变化，世界各国税务部门不断提高自身的信息化建设，以此来紧跟时代的步伐。

1、加大信息化投入

美国国内收入局从 1998 年开始了为期 15 年的现代化重组和改革，包括组织机构重组和信息系统的现代化改造。加拿大全国七大征税中心实行全面联网，并

与海关、银行等部门互联互通。另外，各国还广泛应用电子申报手段，并积极向纳税人推广。

2、重视税收基础管理

多数国家都给纳税人一个唯一的编号，用于税收管理，以利于信息共享和税收状态监控，使纳税人的涉税信息得到充分的对比和分析。

3、纳税服务新手段

西方各国均建立了税务网站，并提供全天候的纳税服务。通过税务网站办理相关税收业务，保证纳税人随时了解和掌握自身的纳税信息。

4、提高涉税数据的分析能力

西方各国大都加强涉税数据的分析能力，并充分利用第三方信息，提高税务审计和选案的准确性。澳大利亚的税务审计人员占整个税务机关人员 10%以上。同时借助涉税数据的分析，对纳税人进行分类管理和防范偷逃避税。

其中美国国内收入局主管信息化部门的是现代化与信息技术服务部，其四个重点工作领域分别是人员和知识的开发与保留、IT 系统环境的简化和现代化、运维的效率和 IT 系统的安全。为实现美国国内收入局改进纳税服务、加强税收征管和提升现代化水平的三大目标，现代化与信息技术服务部肩负着四大使命：改善信息化服务、维护现代化的系统与设备、为资源增值以及改进 IT 安全防护措施。为完成《美国国内收入局战略规划 2009-2013》中的两大战略目标，美国国内收入局要在现代化科技上继续投入。

2006 年 1 月，随着德国联邦税收管理局这个改革项目的执行，联邦税收管理局对已经存在的部门进行了全面的重组，将联邦收入管理局的数据处理和信息技术中心和联邦财政管理局的信息处理部门的职能进行整合，形成联邦税收管理局的数据处理和信息技术中心。它的职能包括：开发、维护特殊软件以及提供 7*24 小时的信息系统基础设施运营。[5]

日本税务部门已经实现了覆盖全国的三级计算机信息网络。各单位信息中心也形成了由若干信息系统构成的信息管理系统。[6]

1.2.2 国外的标准和框架

1、英国

BS 7799 是英国标准协会制定的一个标准。建立的目的就是引导企业建立自身的信息安全管理体系。

第一部分是管理实践规范，后来成为 ISO/IEC 17799:2005 标准的一部分，主要供安全系统开发人员作为参考使用。第二部分是一整套规范，后来成为 ISO/IEC 27001:2005 标准的一部分。

2、ISO/IEC 27000 族

ISO/IEC 27000 族是国际标准化组织关于信息安全管理体系建设的标准总称。该标准族的前九个标准为信息安全管理体系的基本标准，第十至第十九为前九个标准的解释指南与文档。

其中 27001 和 27002 是核心标准。其中， 27001 适用于任何类型的组织机构。27002 涵盖了信息安全的各个方面的措施。它为如何建立、推行、维持及改善信息安全管理系统提供帮助。[7]

3、信息保障技术框架

美国提出的信息保障技术框架，对现有的信息保障焦点问题和实践提供了建议和指南，特别适合于从事信息保障工作的系统安全工程师与相关人员使用。在框架中，信息保障的三要素是指人、技术和操作。3.0 版本中尚未完成预想的内容有多级安全和语言通信。美国曾经提出 4.0 版本的结构建议，目的是形成基于 WEB 的形象工具，使用户可以查找关心的主题和技术细节，可以让用户根据自己的需求生成自己的最小信息保障技术框架。[8]

图 1.2 为美国信息保障技术框架图。

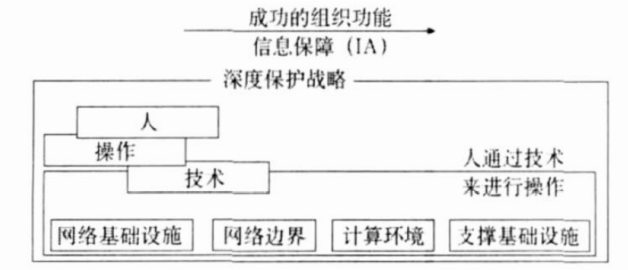

图 1.2 美国信息保障技术框架

来源：虞文进,李健俊著、《信息安全与通信保密》、2010 年 01 期[9]