组织安全保障体系与智能ISMS模型

郭建东 秦志光 刘乃琦

(电子科技大学计算机学院 成都 610054)

【摘要】介绍了ISO7498-2、ISO17799、ISO27001和ISO/IEC18028-2等四个信息安全保障的重要标准的相关内容。针对组织安全问题，提出了一个适合不同组织模型的整体安全保障体系。在该安全保障体系中，把一个组织作为一个整体对象，以整体安全作为组织安全保障的重要措施，构建了一个组织安全保障的过程模型。针对当前信息安全实施中的主要问题，结合信息安全管理系统的概念，提出了一个智能化的组织安全管理体系框架。

关 键 词 体系; 智能; 管理系统; 组织; 安全
中图分类号 TP3 文献标识码 A

Organization Security Architecture and Model of Intelligence ISMS

GUO Jian-dong，QIN Zhi-guang，LIU Nai-qi

(School of Communication Information Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract In this paper, several important standards, including ISO7498-2, ISO17799, ISO27001 and ISO/IEC18028-2, are described. An integrated security ensuring architecture which is adapted to different organization models is proposed in order to solve the problems of organization security. Using the architecture, an organization is looked as an entity and as a whole. Integrated security is the most important method to ensure the security of an organization and a process model is proposed. Combining with the concept of Information Security Management Systems, an intelligent security management framework of organization is proposed also.

Key words architecture; intelligence; ISMS; organization; security

计算环境的高速发展给人类带来了资源和效率，也造成了对各种高度发达的计算技术的依赖，其程度随着计算机和网络技术以及嵌入式终端的发展而在迅速加深，并且不可逆转。人类对计算技术与环境的依赖，是造成信息安全问题的根源。研究人员对信息安全问题开展了大量的研究和开发工作，与信息安全相关的成果不断出现，解决了计算环境的生存问题，但没有给人们带来真正的安全感。

文献[1-2]对中国2000年12月～2006年12月期间接入互联网的计算机数量和新增病毒数量进行了对比。由文献[1-3]提供的数据可以看出：信息安全问题几乎与互联网的发展规模成正比。在当前的计算架构下，安全只能是相对的。目前，在信息安全的研究领域，有三个方面引起广泛关注：(1) 安全的网络而不是网络安全。网络之所以存在安全问题，其根本原因是网络体系本身存在安全漏洞，应该从网络体系着手解决安全问题。(2) 整体安全。将计算环境作为各个大小不同可能存在信息交换关系的局部，对各个局部采取组织、管理、技术等全面的措施，提供信息安全的保障。(3) 智能安全。依靠人工免疫、进化计算、神经网络、群体智能等理论的发展，建立智能安全体系。

1 内网安全问题与组织安全

本文定义一个简化的内网模型为：(1) 可以有或没有与Internet的连接通道；(2) 可以是一个组织内部网络的一部分或者全部；(3) 物理上或者逻辑上的局域网；(4) 网内完成组织的业务，可能需要或不需要进行网外业务数据的交换。

文献[4]把信息安全划分为五个层次：(1) 家庭用户和小企业；(2) 大企业；(3) 重要部门(如联邦政府、州和地方政府、高等教育部门、秘密部门等)；(4) 国家优势；(5) 全球。第(1)~(3)层都涉及内网的安全问题。

文献[5]说明了ISO/IEC18028-2中所给出的安全威胁的定义：(1) 信息或者其他资源的破坏；(2) 信息损坏或者改变；(3) 信息以及其他资源的移除、被

收稿日期：2007－03－25
作者简介：郭建东(1967－)，男，在职博士生，主要从事软件、智能工程与信息安全等方面的研究.

盗或丢失；(4) 信息的泄漏；(5) 服务的中断。

可以把内网的安全问题概括为：(1) 内部资讯的保护；(2) 计算机系统的安全；(3) 与互联网或网外的连接安全；(4) 安全事故的响应。

员工的隐私问题是一个组织建立安全体系时不可回避的问题，不同的组织对此会有不同的认识和政策，但必须面对隐私问题的多样性。组织安全是为了构建安全的组织所采取的全面的技术和管理措施的集合。

2 国际标准保障体系

2.1 ISO7498-2

OSI/RM(ISO7498)所定义的七层模型奠定了网络的基础，但它是一个失败的网络体系，可以概括为以下原因：(1) 标准制订的时机不恰当；(2) 标准分层过多、过细；(3) 重复校验，无效工作太多；(4) 缺乏对网络安全的保障。作为最早的网络体系标准，OSI/RM缺乏对信息安全的正确认识和定义。为了弥补ISO7498在信息安全方面的缺陷，国际标准化组织于1989年12月发布了ISO7498-2，定义了OSI的信息安全体系，即五类服务和八种安全机制。五类服务为：(1) 鉴别服务；(2) 访问控制服务；(3) 数据保密性服务；(4) 数据完整性服务；(5) 抗抵赖性服务。八种安全机制为：(1) 数据加密机制；(2) 数字签名机制；(3) 访问控制权机制；(4) 数据完整性机制；(5) 鉴别交换机制；(6) 业务填充机制；(7) 路由控制机制；(8) 公证机制[6-7]。同样，ISO7498-2对网络与信息安全的内容具有重要的指导意义。

2.2 ISO17799和ISO27001

ISO17799和ISO27001来源于英国标准BS7799，图1为两者与BS7799的关系及其发展历程[8]。ISO17799和ISO27001的目的是构建一个信息安全的管理体系(Information Security Management Systems, ISMS)。

ISO17799是一个得到国际上广泛承认的ISMS实践章程和指导建设ISMS的、全面的框架，也是用于保护企业和组织的国际标准。ISO17799认为信息安全就是保持信息的可信性、完整性和可用性，这是信息安全的根本目标。ISO27001为国际公认的一个ISMS的需求文档，定义了133项安全控制实践的ISMS需求的集合，包括：(1) 安全政策；(2) 信息安全组织；(3) 资产管理；(4) 人力资源安全；(5) 物理和环境安全；(6) 通信和操作管理；(7) 访问控制；(8) 信息系统的收集、开发和维护；(9) 信息安全事件管理；(10) 业务连续性管理；(11) 符合性。

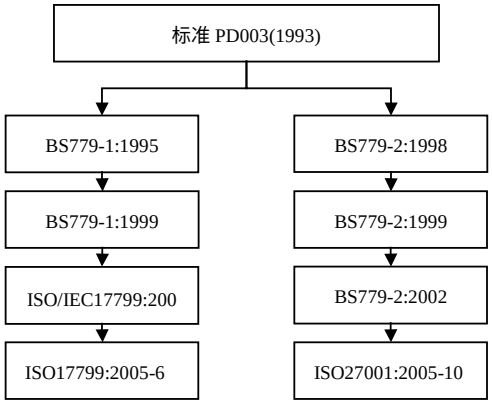

图1　ISO17799和ISO27001的发展历程

2.3 ISO/IEC18028-2

ISO/IEC18028-2[5]定义了一个严谨而且适应广泛的网络安全框架，其框架如图2所示。在这个架构中，通过八个安全维度，定义了一个多层的网络安全视图。框架中把一个网络中所能够采取的安全措施分成三个层次：(1) 基础架构安全层，由处于网络或系统底层的硬件和软件平台组成，用于提供通信网络、服务、应用以及数据传输的连接；(2) 服务安全层，由客户或者端用户所使用的网络安全服务组成，如认证、授权以及VPN等；(3) 应用安全层，提供用户访问的基于网络的应用，如FTP、E-mail、浏览器等。

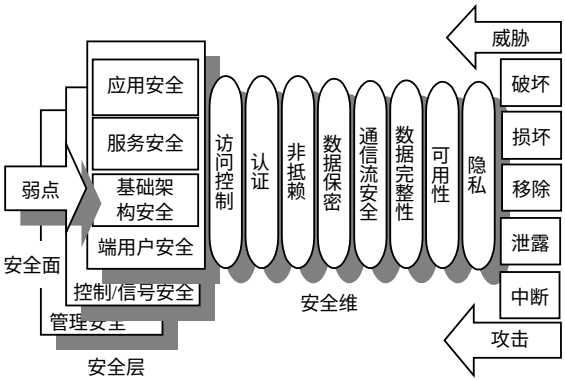

图2　ISO/IEC18028-2安全框架

在ISO18028-2中，把人们在网络上的行为划分成三类，用三个安全平面代表：(1) 管理平面；(2) 控制平面；(3) 端用户平面。每一个平面都会存在安全问题，同一个安全威胁类型也有可能存在于两个或者三个安全平面。

ISO18028-2定义的八个安全维度包含了每一层或者平面针对威胁和攻击所可以采用的技术：(1) 访问控制(Access Control)，提供对网络资源的授权访问；(2) 认证(Authentication)，确认参与通信的各个

实体；(3) 非抵赖(Non-repudiation)，维持审计跟踪信息，保证最初的数据或者事件或行为的发起不能被否认；(4) 数据保密(Data Confidentiality)，保护数据避免未授权的泄露；(5) 通信流安全(Communication Flow Security)，确保信息在授权的端点之间流动而没有被改变方向或截获；(6) 数据完整性(Data Integrity)，维护数据的正确性或精确性，避免未授权的变动、删除、产生和复制；(7) 可用性(Availability)，确保对网络装置、存储信息、信息流、服务和应用的访问不被拒绝；(8) 隐私(Privacy)，保护可能由于对网络行为的监视而被获取的信息。

3 整体化的组织安全模型

3.1 组织的信息环境类别

按照本文所述关于内网的特点，可以把一个组织按照信息环境的特点划分为以下六类：(1) 唯一的局域网，没有互联网相关业务；(2) 唯一的局域网，有互联网相关业务；(3) 多个局域网，无跨地域网络，无互联网相关业务；(4) 多个局域网，无跨地域网络，有互联网相关业务；(5) 多个局域网，有跨地域网络，无互联网相关业务；(6) 多个局域网，有跨地域网络，有互联网相关业务。

从网络的角度看，一个组织的安全包括：(1) 主机安全；(2) 局域网内安全；(3) 局域网间安全；(4) 网络与互联网访问安全；(5) 互联网上的业务安全；(6) 跨地域内部网依赖于互联网的通信业务安全。可以把每一个部分作为组织的一个子信息环境。

不同的组织对待隐私问题会有不同的认识和政策。由于隐私问题在目前的计算环境下，可能会导致组织资讯泄露的主要行为有：(1) 软盘或U盘等移动存储设备的使用；(2) 互联网内容的访问；(3) 网内或网间计算机的通信；(4) OICQ、MSN等即时通信程序的使用；(5) BBS等互联网内容的访问，网络信息的发布；(6) 来自于网络或存储的应用的安装、运行；(7) 电子邮件；(8) FTP等应用层服务的执行。

3.2 组织安全实施过程模型

一个组织的安全体系可以划分为组织安全管理体系和组织安全技术保障体系两个部分。

根据ISO7498-2、ISO17799和ISO27001的内容，可以把组织安全保障所包括的内容概括如下：(1) 安全管理组织机构建设；(2) 信息安全政策制订；(3) 信息资产评估；(4) 技术和政策保障措施的实施；(5) 安全事件应急响应；(6) 安全体系的改进；(7) 安全水平评估。

图3所示的一个组织安全保障过程是一个闭环过程模型。由于计算技术的发展与组织的变动，不可能得到一个绝对安全的组织计算环境，也不可能避免安全事件的发生。一个有效的组织安全体系应该做到把安全事件所造成的影响限制在最小，而且具备对组织变化和安全事件的快速反应能力。

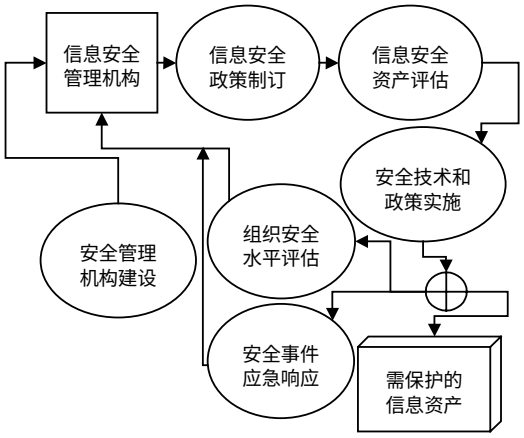

图3 组织安全保障过程模型

在一个组织安全体系中，所涉及的主要对象包括：(1) 信息安全管理机构；(2) 信息安全政策；(3) 信息安全的技术保障措施；(4) 信息安全资产；(5) 信息安全事件。

4 智能化的ISMS实现

ISO17799和ISO27001对ISMS的概念和需求给出了详细的说明，对ISMS具有重要的指导意义。信息安全管理系统可以定义为一个“为了信息建立和维护一个安全的环境的管理系统”[9]。一个严谨的组织安全体系是其安全管理体系和技术体系的合成。

在近年的信息安全科学发展的过程中，存在以下问题：(1) 片面依赖设备和技术。安全领域所取得的成果主要体现在防病毒软件、防火墙、IDS等安全设备和系统上，这些设备和系统的使用保证了一个组织业务的正常运行，但是忽略了管理的作用。虽然有ISO17799和ISO27001的推广，很多组织已经认识到了管理的价值，但是缺乏一种自动化和有效的实现体制。(2) 被动防御和事后反应。目前，几乎所有的软件和硬件设备在实现安全措施上都是被动的，防病毒软件采取的方法是在互联网上对病毒的特征码进行在线更新，而硬件设备几乎对新出现的威胁束手无策。

传统的算法解决安全领域的问题面临着有效性和计算效率的问题，防病毒软件中的特征码匹配，

一次杀毒过程需要运行2～3 h。解决安全系统与设备的有效性和效率问题是目前信息安全领域的重要课题。

计算智能的高速发展为信息安全领域的问题提供了一个重要的途径，具有代表性的是人工免疫在计算机滥用和攻击检测中的应用研究[10]。智能算法解决安全问题的研究可以概括为各种问题和威胁的识别，主要包括：(1) 网络威胁和攻击；(2) 病毒和恶意代码；(3) 主机恶意行为(数据泄露)；(4) 主机安全趋势判定；(5) 垃圾邮件；(6) 限制性信息；(7) 安全事件的分析等。

根据组织安全的需求以及ISO17799和ISO27001的内容，在一个ISMS中应该实现的功能需要考虑以下问题：1) 管理政策和流程的实现。通过该功能，ISMS应该克服管理和技术的脱节，把二者融为一体，形成一个完整的组织安全保障体系。2) 一体化的技术保障体系。组织内所采取的技术保障措施应该能够协同工作，以保证这些技术措施的有效性和降低成本。需要克服协同工作的标准和第三方技术的融合问题。3) 智能化的安全体系。对安全中的关键问题，采用智能计算技术和传统方法相结合，实现对安全威胁和信息的自动识别，提高系统保障的有效性。4) 隐私政策的多样性。不同的组织类型对隐私问题会有不同的政策。该ISMS应该具有很高的配置能力，以保证足够的适应性，包括以下几个子系统：(1) 安全政策的发布和管理；(2) 安全事件的记录和响应；(3) 主机安全系统；(4) 服务器安全系统；(5) 网外通信管理；(6) UTM设备。

在每一个子系统中，根据组织的需求，实现内部的安全政策和威胁的控制，同时利用软件技术依靠整个系统实现反馈。

5 结 束 语

ISO7498-2是对OSI七层模型的重要补充，所提出的安全服务和安全机制的概念，对实现安全的计算环境具有重要的指导意义。ISO17799和ISO27001提出了ISMS的需求和组织安全水平的评估标准，是实现组织安全体系的重要指南。通过一个软件系统，结合现代智能计算的研究，实现组织的安全管理和技术体系的自动化，真正实现三个安全标准的内容，具有重要的应用价值。

参 考 文 献

[1] 中国互联网络信息中心. 中国互联网发展报告[EB/OL]. http://www.cnnic.com.cn/html/Dir/2007/07/17/4722.html, 2007-01-22.

[2] 金山软件有限公司. 中国互联网2006年信息安全报告[EB/OL]. http://www.cqvip.com/qk/85981X/200704A/24315804. html, 2007-01-16.

[3] Symantec Corp. Internet security threat report-trends for January 06-June06[EB/OL]. http://www.portal.acm.org/, 2006-08-20.

[4] The President’s critical infrastructure protection board. The national strategy to secure cyberspace for comment (draft) [EB/OL].www.bespacific.com/mt/archives/000108. html, 2002-09-18.

[5] SABNIS S, CHANDRASHEKHAR U, BASTRY F. Challenges of securing an enterprise and meeting regulatory mandates[C]//12th International Telecommunications Network Strategy and Planning Symposium. [S.l.]: IEEE, 2006: 1-6.

[6] GRAFT D, PABRAI M, PABRAI U. Methodology for network security design[C]//Computers and Communications, Ninth Annual International Phoenix Conference. Scottsdale, AZ, USA: IEEE, 1990: 675-682.

[7] SHAW G. NATO OSI security architecture[C]//IEE Colloquium on Security and Networks. London, UK: [s.n.], 1990.

[8] SQM-ADVISORS, LLC. Executive briefing on ISO17799: 2005 & ISO27001:2005[S]. http://www.sqm-advisors.com/download1.html, 2006.

[9] SANCHEZ L E, VILLAFRANCA D, FERNANDEZ-MEDINA E, et al. Practical approach of a secure management system based on ISO/IEC 17799[C]//Availability, Reliability and Security(ARES 2006). Washington D C, USA: IEEE Computer Society, 2006: 585-592.

[10] IDRIS N B, SHANMUGAM B. Artificial intelligence techniques applied to intrusion detection[C]//INDICON, 2005 Annual IEEE. [S.l.]: IEEE, 2005.

编 辑 黄 莘