IBM
管理顾问丛书

信息安全战

企业信息安全建设之道

新技术带来安全隐患

互联网时代

如何保护我们迫在眉睫的信息安全

内附：企业信息安全框架

余磊　杨斌　李遥　谢海涛　高峰　著

Enterprise Security Framework

出版社

信息安全战

企业信息安全建设之道

余磊　杨斌　李遥　谢海涛　高峰　著

東方出版社

图书在版编目（CIP）数据

信息安全战：企业信息安全建设之道/余磊 等著. —北京：东方出版社，2010
ISBN 978-7-5060-3844-7

Ⅰ. 信… Ⅱ. 余… Ⅲ. 企业管理—管理信息系统—安全技术 Ⅳ. F270.7

中国版本图书馆 CIP 数据核字（2010）第 038017 号

信息安全战：企业信息安全建设之道

作　　者：余　磊　杨　斌　李　遥　谢海涛　高　峰
责任编辑：姬　利　陈景雷
出　　版：东方出版社
发　　行：东方出版社　东方音像电子出版社
地　　址：北京市东城区朝阳门内大街 166 号
邮政编码：100706
印　　刷：北京智力达印刷有限公司
版　　次：2010 年 4 月第 1 版
印　　次：2010 年 4 月第 1 次印刷
开　　本：787 毫米×1092 毫米　1/16
印　　张：13.5
字　　数：143 千字
书　　号：ISBN 978-7-5060-3844-7
定　　价：32.00 元
发行电话：（010）65257256　65245857　65276861
团购电话：（010）65230553

序言一

在“智慧的地球”这一颇具包容性理念的指引下，客户的业务将以一种更为精细和动态的方式进行。 在“智慧的地球”上，各个领域的边界将会逐渐地溶解，各个领域之间交互的信息量激增，且必将建立在更加信任的基础上。 与此同时，随“智慧的地球”孕育而生的新的协作方式将导致信息的流转变得更为复杂。 这些都为企业在新的全球化环境中的生存和发展带来新的风险和挑战。

IBM 提出“企业信息安全框架”（ESF，Enterprise Security Framework V5.0）的核心目的是，在 IT 系统已经成为企业业务的运营平台之际，如何在企业无比复杂的信息环境中，对企业的信息安全进行整体的、全面的把控。

“整体安全”的概念在安全业界已经不再是一个生疏的话题，IBM 的企业信息安全框架（ESF）的创新意义在于，首次从企业的业务本身出发，结合安全最佳标准和业界相关标准的安全模型，形成一套行之有效的方法论，帮助企业定位安全建设的现状、了解安全建设的需求、组织未来安全建设的规划和实施。

众所周知，即便是在信息安全国际标准和相关最佳实践的指导下，企业按照标准的安全实践方法，设计和实施信息安全解决方案时，依然会遇到很多挑战。企业还必须考虑多平台、多组件架构集成的复杂性、实施安全解决方案的多样性等。

那么，企业信息安全框架（ESF）是如何能做到行之有效的呢？ 企业信息安全框架（ESF）所提供的又是怎样的一个安全模型呢？

行之有效的最根本原因是，企业信息安全框架（ESF）指导企业在信息安全建设之初，即根据企业业务发展的需要，确立合理的信息安全需求、确立企业信

息安全架构，根据企业的实际和需要选择安全功能组件。

企业信息安全框架从上到下由三个主要层次组成：“安全治理、风险管理和合规层”、“安全运维层”、“基础安全服务和架构层”。安全治理、风险管理和合规层，是后两者的理论依据；安全运维层，则是对安全生命周期全过程的管理；基础安全服务和架构层，是企业信息安全建设技术需求和功能的实现者。

（1）全治理、风险管理和合规

它处于企业信息安全框架的最顶层，是业务驱动安全的出发点。主要包括企业战略和治理框架、风险管理框架、合规和策略遵从。通过对企业业务和运营风险的评估，确定其战略和治理框架、风险管理框架，定义合规和策略遵从，确立信息安全文档管理体系。

（2）安全运维

安全运维是指在安全策略的指导下，安全组织利用安全技术来达成安全保护目标的过程。主要包括安全事件监控、安全事件响应、安全事件审计、安全策略管理、安全绩效管理、安全外包服务。安全运维与IT运维相辅相成、互为依托、共享资源与信息，它与安全组织紧密联系，融合在业务管理和IT管理体系中。

（3）基础安全服务和架构

基础安全服务和架构定义了企业信息安全框架中的五个核心的基础技术架构和相关服务：物理安全、基础架构安全、身份/访问安全、数据安全和应用安全。基础安全服务和架构是安全运维和管理的对象，其功能由各自子系统提供保证。

总之，企业信息安全框架（ESF V5.0）给企业信息安全建设提供了一个集成的、标准的企业信息安全框架，帮助企业快速知晓企业信息安全现状和需求，能为企业信息安全平台的建设、设计、实施提供指导和参照，从而使业界提出多年的企业“整体安全”理论能够真正落地。

目前业界有很多关于信息安全建设的资料和书籍，但绝大多数都是针对安全建设具体技术的探讨。本书旨在帮助企业的高级管理层从风险管控的角度出发，从战略的高度全方位地考虑和实施安全的整体框架，实现一个风险可控的、优化的业务信息支撑体系。

易博纳（Bernard Elharrar）
IBM大中华区全球信息科技服务部总经理

序言二

早在2006年，国家信息化小组就已在《2006—2020年信息化发展战略》报告中明确提出，信息技术的快速发展必将带动一场新的全球产业革命，我们必须深刻地认识到这一变化带来的机遇和挑战。

时代步入了一个科技创新不断涌现的重要时期，党中央、国务院一贯坚持创新，推动了我国信息产业和信息化建设的发展，使得信息网络技术的应用得到了迅速普及。 近年来，我国信息化应用水平持续、快速发展，信息化在促进经济发展、调整经济结构、改造传统产业和提高人民生活质量等方面发挥了不可替代的重要作用。

如今，信息技术的应用早已涵盖了绝大多数党政部门、金融、税务、海关、水利、交通等重要业务领域的业务系统和企业管理信息系统。 可以说，我国已经成为一个屹立在东方的信息化大国。

与此同时，我们也必须清醒地看到，随着我国信息化的高速发展，信息系统已经成为我国众多行业和领域的神经中枢，信息系统的安全直接影响到这些行业和领域的日常工作和生产的正常运转，信息系统的可靠性和安全性将直接关系到政府、企业及其他行业的生存力和竞争力。 因此，信息系统的安全已经成为信息化进一步发展过程中必须考虑和解决的重要问题之一。

对于国家而言，信息安全体系建设是我们在“十一五”期间必须完成的重要任务之一。 我们国家需要提高的六项能力，就是安全防护能力、安全监管能力、应急响应能力、信息对抗能力、评估能力、信任保护能力。 同时我们要加大力度自主研发信息安全的关键技术和设备，满足国家对信息安全的要求，要在

密码技术、网络信任技术、可信安全计算技术、网络监管技术等方面达到国际领先水平，要在安全监管、安全评估等方面达到世界先进水平。

对于企业而言，进行信息安全建设和规划，要研究建设信息安全的综合成本与信息安全风险之间的平衡，而不是片面追求不切实际的安全。 不同的行业、不同的应用甚至同一个企业的不同部门，对于信息安全的要求都有所不同，信息安全建设并不是“越安全越好”。 面对全球一体化的互联网环境，企业如何提高安全防护和保障能力，是摆在 CIO 面前的巨大难题。

长期以来，我国众多行业和领域的信息化安全建设存在着“重产品、轻体系”的怪圈，企业每年投入大量的人力、物力采购信息安全产品，但信息系统的管理者们仍处于“信息安全年年建，安全问题年年有”的窘境之中。 究其原因，是因为体系化的信息安全建设这一指导原则没有得到足够的宣传和普及。

在国家层面重视信息化安全体系建设这个大好前景下，IBM 公司从国内信息安全建设的现状出发，结合其在全球信息安全建设方面的经验和实践，提出了“企业信息安全框架”这一长治久安的信息安全建设总体思路，为各行各业的企业信息系统管理者们进一步建设可靠的信息安全保障系统提供了系统的指引和参考。

相信广大的企业信息系统管理者们，一定能借助本书提供的方法和理论，全局性地审视自身信息安全体系的不足，找到适合企业需要的信息安全建设的破局之路。

宁家骏

国家信息化专家咨询委员会委员

2010 年 2 月 26 日

目录

上篇

风起云涌，危机四伏

第一章
“信息生态”已经改变

信息网络产业是世界经济复苏的重要驱动力。全球互联网正在向下一代升级，传感网和物联网方兴未艾。“智慧地球”简单说来就是物联网与互联网的结合，就是传感网在基础设施和服务领域的广泛应用。我在无锡考察时参观了中国科学院微系统所无锡传感网工程中心，很高兴看到一批年轻人正在从事传感网的研究。我相信他们一定能够创造出“感知中国”，在传感世界中拥有中国人自己的一席之地。我们要着力突破传感网、物联网的关键技术，及早部署后 IP 时代的相关技术研发，使信息网络产业成为推动产业升级、迈向信息社会的“发动机”。

——摘自　温家宝在首都科技界大会上的讲话　2009 年 11 月 3 日

一、智慧的地球

随着信息技术在全球的发展与应用，世界正变得更“平”、更“小”，与此同时，身处其中的企业却面临着金融危机、气候变暖、恐怖主义、能源紧张、环境污染等各种严峻挑战，日益融为一体的世界使我们面临各种全球问题。但幸运的是，有一股新的力量正在兴起，并通过以下几个方面的改变赋予人们能力，使人们能越来越智慧地解决这些问题。

首先，各种创新的感应科技开始被应用于各种物品和设施中，从而令物质世界被极大程度地数据化了。

其次，随着网络的高度发达，人、数据和其他各种事物都将以不同方式联入网络。

先进的技术和超级计算机可以对堆积如山的数据进行整理、加工和分析，将生硬的数据转化成实实在在的分析结果和信息，并帮助人们做出正确的行动决策。

这意味着全球数字的和有形的基础架构正在逐渐融合，事实上，几乎所有的事物——任何人、任何物体、任何流程、任何服务或任何组织（不管规模大小）都将牵涉其中。 世界的基础结构正在向“智慧”的方向发展。 可感应、可度量的信息源无处不在，互联网的平台让这一切互联互通，让一切变得更加智能化，世界的基础结构正在向“智慧”的方向发展。

这不只是一个比喻，全球移动电话用户数量早在 2007 年就已突破 33 亿大关，也就是说，全球平均每两个人就拥有一部移动电话。 更重要的是，根据预测，2009 年移动互联网用户的数量将会达到 10 亿之多。 到 2010 年，全球晶体管数量将达到每个人平均占有 10 亿个。 到 2011 年全球上网人数将达到 20 亿人。 到 2010 年，全球生产的射频识别（RFID）数量可望达到 300 亿个，产品、护照、建筑物甚至动物身上都可以配备射频识别。

智慧化不只是实现“无所不在的连接”（pervasive connectivity）。 大规模计算机集群首次具备了用于处理、建模、预测和分析任何工作负载和任务的经济可行性。 作为一种连接和提供具有强大、大规模可扩展后端系统的庞大最终用户设备、传感器和致动器阵列的方法，“云计算”开始进入人们的视野。 利用云计算技术可以快速开发新型应用并将其部署为网络服务。 基本计算模式在过去 20 年中已经发生了变化。 20 世纪 80 年代出现的个人电脑模式已被目前基于开放性、网络、高新技术以及数字智能与工作和生活相融合的新模式所取代。

这一切都意味着，科技的发展使人类历史上第一次出现了几乎任何系统都可以实现数字量化和互联的事实，并且在此基础上我们能够作出更加智慧的判断和处理。

这也就意味着，经济可行的智能技术将被应用到几乎所有的行业，应用于各种产品，催生过去无法实现的服务。 在此基础上，无论是自然体系，还是行业系统或者企业，甚至人类本身，都将更紧密地相互关联、整合，形成各种各样的智慧系统。

你将会了解到摆在餐桌上的食物来自哪块土地、运输过程中经过了哪些环节；你可以随时了解城市的交通状况，从而及时调整出行路线；去医院看病时，无需再排长队、奔波于各个窗口之间；厨房里的自来水也可以放心饮用，因为你

知道水的整个输送过程都在被严密监测着……

“智慧的地球”是我们共同的诉求。不论是企业、政府、学界，还是个人，都希望获得新的洞察能力，都追求绿色可持续发展。大家都希望能够聪明地运作，将整个社会生活建立在灵活而动态的基础设施之上。“智慧的地球”，能够让世界变得更加美好。

世界将继续“缩小”、“扁平化”和变得“智慧”，问题是，面对这一现实的我们需要做些什么？我们正处于一个重要的科学探索新纪元的黎明前夕，有许多事情有待被发现和理解——从物理学和材料科学到生物化学，再到数学和分析学。这些飞速发展的现实，已经向我们提出了一个更加值得关注的问题：我们在未来十年和更长时间内应当如何投资、合作、转变我们的组织架构或管理我们自身？

二、物联网

物联网（the Internet of things）的概念最早出现在1999年。顾名思义，物联网就是“物物相联的互联网”。这有两层意思：第一，物联网的核心和基础仍然是互联网，是在互联网基础上延伸和扩展的网络；第二，其用户端延伸和扩展到了任何物品与物品之间，进行信息交换和通讯。严格而言，物联网的定义是：通过射频识别（RFID）、红外感应器、全球定位系统、激光扫描器等信息传感设备，按约定的协议，把任何物品与互联网连接起来，进行信息交换和通讯，以实现智能化识别、定位、跟踪、监控和管理的一种网络。

国际电信联盟2005年的一份报告曾描绘物联网时代的图景：当司机出现操作失误时，汽车会自动报警；公文包会提醒主人忘带什么东西了；衣服会“告诉”洗衣机对颜色和水温的要求等等。这种情景并不遥远，就在不久前，无锡传感网工程中心的传感器产品在上海浦东国际机场和上海世博会被成功应用。这套设备由10万个微小的传感器组成，散布在墙头、墙角、墙面和周围道路上。传感器能根据声音、图像、震动频率等信息分析、判断爬上墙的究竟是人还是猫、狗等动物。

统计显示，全球联网对象——亦即构成物联网的车辆、设备、摄像头、车道、管道——的数量正在迈向1万亿大关。美国权威咨询机构Forrester预测，到2020年，世界上“物物互联”的业务，跟“人与人通信”的业务相比将达到30比1。

物联网用途广泛，遍及智能交通、环境保护、政府工作、公共安全、平安家居、智能消防、工业监测、老人护理、个人健康等多个领域。预计物联网是继计算机、互联网和移动通信网之后的又一次信息产业浪潮。有专家预测10年内物联网就可能大规模普及，这一技术将会发展成为一个具有上万亿美元规模的高科技市场。

物联网中非常重要的技术是电子标签技术（即射频识别技术，RFID），它可以结合已有的网络技术、数据库技术、中间件技术等，构筑一个由大量联网的阅读器和无数移动的标签组成的、比Internet更为庞大的物联网。

物联网把新一代IT技术充分运用在各行各业之中，具体地说，就是把感应器嵌入和装备到电网、铁路、桥梁、隧道、公路、建筑物、供水系统、大坝、油气管道等各种物体中，然后将物联网与现有的互联网整合起来，实现人类社会与物理系统的整合。在这个整合的网络当中，核心系统是处理能力超级强大的中心计算机群，能够对整合网络内的人员、机器、设备和基础设施实施实时的管理和控制，在此基础上，人类可以以更加精细和动态的方式管理生产和生活，达到“智慧”状态，提高资源利用率和生产力水平，改善人与自然间的关系。

毫无疑问，如果物联网时代来临，人们的日常生活将发生翻天覆地的变化。

三、新技术，新风险

物联网为我们带来了更平、更小、更智慧的地球，使我们的联系和信息传递更加紧密，互联互通程度更高。新的技术带来了数十亿计的移动设备、实时的信息交流以及更加紧密、更加多样化的协作方式，这些新技术的大规模应用一方面提供了智慧的能力，另一方面也带来了新的风险。

云计算作为这些新兴技术中的代表，是随着处理器技术、虚拟化技术、分布式存储技术、宽带互联网技术和自动化管理技术等的综合发展而产生的，这一大规模的计算能力通常是由分布式的大规模集群和服务器虚拟化软件搭建而成的。

对于云计算的使用者而言，云计算提供了无限的规模和差异化的服务，简化了服务的交付。特别是在智慧地球、物联网这样的大背景下，许多企业希望、也需要通过云计算培养快速创新和制定决策的能力，以便可以在当今高度竞争的环境中快速地作出应对，同时还通过云计算降低资金和运营成本。此外，云计算还提供了一个可伸缩的环境，以便轻松有效地满足客户的需要。

在国内，对“云计算”的研究也逐渐增多。各种“云计算”研究、云技术

论坛频繁活动。2008 年，中国电子学会还专门成立了云计算专家委员会。为了清晰掌握中国企业用户对于云计算的态度，很多媒体和分析机构也作了相关的调研。

在云计算带来创新能力、创造众多市场机会的同时，分析师们还没有忘记提醒用户“云计算有风险，入云需谨慎”。为此，研究机构 Gartner 在 2008 年年中发布了一份名为《云计算安全风险评估》的报告。报告指出，云计算需要进行安全风险评估的领域包括数据完整性、数据恢复及隐私等。此外，还需对电子检索、可监管性及审计问题进行法律方面的评价。报告同时列出了云计算技术面临的 7 大风险，包括：特权用户的接入、可审查性、数据位置、数据隔离、数据恢复、调查支持、长期生存性。

同时，2009 年发生的几件有关云计算的事件，也让众多用户对云计算现在的不稳定性增添了一些顾虑。例如，在 2009 年 3 月中旬，微软在 2008 年专业开发者大会上推出的云计算版本操作系统 Windows Azure 完全断线，其提供的在线服务包括 SQL-NET、Live、SharePoint、Dynamics CRM 等均无法使用。虽然 Windows Azure 仍处于测试阶段，但是在一些企业用户体验之后，仍然对其背后的安全性能等问题存在诸多顾虑。

2009 年 9 月下旬，Google 又爆出 Gmail 断网事件，虽然这次只影响到一小部分用户，但事实上 Google 已经多次出现类似问题，这些问题多被认为和 Google 云服务的不稳定有关。Google 已不满足于搜索引擎等网络服务，转而大力发展云服务，试图开发大企业客户的网络办公平台。虽然 Google 的云服务具有方便、简易、效率高等优点，但频繁发生的断网事件，让人着实怀疑其稳定性。这也将极大影响 Google 云战略的未来。

可以看到，新生事物和技术的出现，必将带来新的问题和风险，如何在有效利用新技术的同时，及时识别和规避这些风险，是一个需要我们长期关注、不断探索的问题。