电力企业信息安全培训系列丛书

信息安全基础知识

XINXI ANQUAN
JICHU ZHISHI

中国电力科学研究院 编

中国电力出版社
CHINA ELECTRIC POWER PRESS

电力企业信息安全培训系列丛书

信息安全基础知识

XINXI ANQUAN
JICHU ZHISHI

中国电力科学研究院　编

中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

本书紧扣电力企业信息安全工作的实际需要，主要介绍了信息安全理论基础、技术知识和业务实操等方面的内容。全书共4章，主要内容包括信息安全法律法规与标准、信息安全管理、信息安全技术和电力企业信息安全工作指南。

本书体系完整，结构清晰，难度适中，可作为电力企业各类信息安全培训及考试人员的参考书，也可作为电力企业和其他大型企业信息安全管理人员和技术人员的实践指导。

图书在版编目（CIP）数据

信息安全基础知识 / 中国电力科学研究院编. —北京：中国电力出版社，2011.12
（电力企业信息安全培训系列丛书）
ISBN 978-7-5123-2548-7

Ⅰ. ①信… Ⅱ. ①中… Ⅲ. ①电力工业－工业企业－信息系统－安全技术－中国 Ⅳ. ①F426.61

中国版本图书馆CIP数据核字（2011）第279000号

中国电力出版社出版、发行
（北京市东城区北京站西街19号 100005 http://www.cepp.sgcc.com.cn）
汇鑫印务有限公司印刷
各地新华书店经售
*
2012年11月第一版 2012年11月北京第一次印刷
787毫米×1092毫米 16开本 12印张 260千字
印数 0001—3000册 定价 **38.00** 元

前　言

随着信息技术在各电力企业的广泛应用，电力企业信息化程度越来越高，对信息技术的依赖程度越来越大，网络与信息系统的基础性作用日益增强，信息安全已经成为促进信息化进一步深入、保障信息化成果的重要手段，也成为电力安全和国家安全的重要组成部分。在这种背景下，对信息安全管理理论，技术知识和实践操作的全面了解和掌握，成为电力企业的信息化从业人员，尤其是信息安全管理和技术人员的迫切需求。

本书结合近年来在电力行业信息安全领域的大量实际工作经验，详细介绍了电力企业信息安全管理和技术工作中所涉及的各个方面的问题。全书共 4 章。

第 1 章介绍了信息安全法律法规与标准，包括国际信息安全标准规范、我国信息安全标准规范和相关法律法规等；第 2 章从组织机构、安全策略、人员管理、资产管理等方面介绍了信息安全管理方面的知识，并着重阐述了应急响应管理、信息安全工程和安全监理等领域的内容；第 3 章主要内容为信息安全技术，包括物理安全、网络安全、系统安全、应用和数据安全知识，还对信息安全技术相关的密码学基础、安全攻防等领域的内容进行了介绍；第 4 章为电力企业信息安全工作指南，结合电力行业当前的工作重点，对电力企业的信息安全等级保护流程和风险评估方法进行了详细介绍。

本书体系完整，结构清晰，难度适中，可以作为电力企业各类信息安全培训及考试人员的参考资料；同时它也可作为电力企业和其他大型企业信息安全管理人员和技术人员的实践指导。

本书主要编写人员有高昆仑，参加本书编写工作的还有郑晓昆、徐志博、詹雄、李凌、宋晓芹、刘楠、郝增帅、赵婷、梁潇等。彭澎对全书进行了审阅并对部分内容进行了修改，在此表示感谢。本书在编写过程中，参考了大量资料，并得到多位同行的大力支持和帮助，在此表示感谢。

编　者

2012 年 8 月

目　录

1 信息安全法律法规与标准

没有规矩，不成方圆，信息安全能取得成就，是与相关“规矩”的不断建立和完善分不开的，这些“规矩”大致可分为法律、法规、标准、道德等。

法律法规，是指国家按照统治阶级的利益和意志制定、认可，并有国家强制力保障其实施的行为规范的总和，是人类在社会活动中必须遵守的纪律，触犯了就要受到惩罚。简单地说，法律法规是人从事设备活动所不能逾越的行为底线。因此，社会中的每一个人都应该学习信息安全的法律法规，自觉遵纪守法。

信息安全法律法规是法律体系的组成部分。信息安全法律包括强行性和任意性的法律规范。它是由国家强制力来保证实施的，对我国所有公民都具有约束力、任何人都必须遵守。

不同于法律法规的国家执行力保障特性，标准是为在一定范围内获得最优秩序，对活动或其结果规定共同的和重复使用的规则、导则或特性的文件。该文件经协商一致制定并经一个公认机构的批准。标准应以科学、技术和经验的综合成果为基础，以促进最佳社会效益为目的。推行标准化是为了满足建设社会主义市场经济最佳秩序的需求，促进技术进步，提高产品、过程和服务的质量，保证安全和环境卫生，使使用和消费合理化，使商品流通简便和公平，促进工业技术水平的提高，促进对外贸易、经济、技术交流，以适应社会主义市场经济的发展和满足对外经济关系的要求。

信息安全标准是确保信息安全产品和系统在设计、研发、生产、建设、使用、测评中保持一致性、可靠性、可控性、先进性的技术规范和技术依据。通过自主开发的信息安全标准，才能构造出自主可控的信息安全保障体系。信息安全标准是我国信息安全保障体系的重要组成部分，是政府进行宏观管理的重要依据。

1.1 国际信息安全标准规范

1.1.1 国际信息化标准组织

一、国际电工委员会 IEC

国际电工委员会（International Electro technical Commission，IEC）成立于 1906 年，是世界上成立最早的非政府性国际电工标准化机构，IEC 的宗旨是促进电工标准的国际化统一，电气、电子工程领域中标准化及有关方面的国际合作，增进国际间的相互了解。

为实现这一目的，出版包括国际标准在内的各种出版物，并希望各个国家委员会在其国家条件许可的情况下，使用这些国际标准。IEC 的工作领域包括了电力、电子、电信和原子能方面的电工技术。为了推动智能电网建设，IEC 标准化管理委员会（Standardization Management Board，SMB）组织成立了第三战略工作组——智能电网国际战略工作组（Strategy Group 3: Smart Grid）。

IEC 的多个委员会及其下属工作组都在从事信息安全方面标准化工作，如 TC56 可靠性委员会、TC77 电磁兼容委员会、TC108 音频/视频、信息技术和通信技术电子设备的安全委员会、TC65 工业过程测量、控制与制动化委员会下属的 WG10 工业过程测量与控制—网络与系统安全工作组和 TC57 电力系统管理与相关信息交换委员会下属的 WG15 数据与通信安全工作组等。

二、国际标准化组织 ISO

国际标准化组织（International Organization for Standardization，ISO）成立于 1946 年 10 月，是一个全球性的非政府组织，是最大的国际标准制定与发布组织。ISO 的宗旨是在世界范围内促进标准化工作的发展，以利于国际物资交流和互助，并扩大知识、科学、技术和经济方面的合作。主要任务是制定国际标准、协调世界范围内的标准化工作，与其他国际性组织合作研究有关标准化问题。1976 年 IEC 和 ISO 两个组织签订协议，确认 IEC 与 ISO 是两个互为补充的国际组织，共同建立国际标准化体系，并建立密切联系和合作关系。

为更好协作和共同规范信息技术领域，ISO 和 IEC 成立了联合技术委员会，即 ISO/IEC JTC1 信息技术标准化委员会，负责信息技术领域的标准化工作，其下属 SC27 安全技术分委员会的前身是 SC20 数据加密技术分委员会，主要从事信息技术安全的一般方法和技术的标准化工作。

SC27 子委员会分为以下五个工作组：

（1）WG01：信息安全管理体系。

（2）WG02：密码学与安全机制。

（3）WG03：安全评估准则。

（4）WG04：安全控制与服务。

（5）WG05：标识管理与隐私技术。

SC27 所制定的信息安全标准在电力工业信息安全方面也有着重要的影响，尤其是 ISO/IEC 27000 系列标准和 ISO/IEC 15408 在电力企业的信息安全管理和电力系统安全性测评方面有着广泛地应用。

三、电气电子工程师协会 IEEE

电气与电子工程师协会（Institute of Electrical and Electronics Engineers，IEEE）是世界最大的专业性学会，于 1998 年成立标准协会（IEEE-SA），其标准制定内容涵盖信息技术、通信、电力和能源等多个领域，IEEE-SA 已日益成为新兴技术领域标准的核心来源。目前，IEEE 标准协会已经制定了 900 多个现行工业标准，如众所周知的 IEEE 802 有线与无线网络通信标准和 IEEE 1394 标准。IEEE-SA 在信息安全方面的主要贡献是制

定了无线网络安全方面的诸多标准。目前，已发布的信息安全标准有 802.10A《可通用的局域网/城域网安全》、802.10E《IEEE 802 LANs V2.0 中的安全数据交换次级层管理》等。另外，IEEE 于 2009 年 5 月成立了专门工作组，致力于制定一套智能电网的标准和互通原则（IEEE P2030），涵盖电力工程、信息技术和互通协议三个方面的标准和原则；制定互通入网过程的标准，如各个能量源头如何与整个智能电网连接，计量设备的接入（如电能表）和时间同步性等标准。

四、Internet 工程任务组 IETF

Internet 工程任务组（Internet Engineering Task Force，IETF）成立于 1986 年底，是全球互联网最具权威的技术标准化组织，主要任务是负责互联网相关技术规范的研发和制定，当前绝大多数国际互联网技术标准出自 IETF。IETF 在应用、互联网、运行与管理、实时应用与架构、路由、安全、传输和其他这 8 个领域进行标准化研究和制定工作，大部分标准制定工作都是由工作组来完成的，截止到 2006 年 9 月 IETF 共成立了 115 个工作组。

目前，IETF 在安全领域有 15 个活跃的工作组，主要负责研究互联网中的授权、认证、审计等与私密性保护有关的协议与标准，主要成果有 IPSec、TLS、STIME、IKE 和 MSEC 等。

五、国际电信联盟 ITU

国际电信联盟（International Telecommunication Union，ITU）是联合国的一个专门机构，也是联合国机构中历史最长的一个国际组织，简称“国际电联”或“电联”。1865 年 5 月 17 日成立时定名为“国际电报联盟”，在 1932 年更名为“国际电信联盟”。ITU 的宗旨和任务是保持并扩大国际合作，以改进和合理使用各种电信手段；促进技术设施的发展和应用，以提高电信业务效率；研究制定和出版国际电信标准并促进其应用；协调各国在电信领域的活动；促进并提供对发展中国家的技术援助。

ITU 下属电信标准化组织（Telecommunication Standardization Sector，ITU-T）是国际电信联盟管理下的专门制定远程通信相关国际标准的组织。ITU-T 的通信安全研究与标准制定工作可以追溯到 2000 年，但直到 2004 年，ITU-T 下属的 SG17 才将标准工作重心转移到通信安全研究上，2009 年 SG17 的研究主题定为通信安全。SG17 下属网络与信息安全、应用安全和标识管理与语言三个工作组，目前，从事包括通信系统安全项目、安全架构与框架、通信信息系统管理、信息安全、垃圾邮件的技术解决方法、安全应用服务和标识管理架构与机制等 12 个安全相关方向的研究工作。目前，已经发布的标准包括《ITU-TX.1121 移动端到端数据通信安全技术框架》、《ITU-TX.1121 基于 PKI 实施安全移动系统指南》、《ITU-TX.1081 远程生物识别多模式模型——远程生物识别安全规范框架》、《ITU-TX.1051 信息安全管理系统——通信需求（ISMS-T）》和开放系统互联的安全（X.800-X.849）等。

1.1.2 美国信息化标准组织

一、美国国家标准学会 ANSI

美国国家标准学会是美国自愿性标准组织的管理和协调机构，总部设在纽约，共有

250 多个专业学会、协会、消费者组织以及 1000 多个公司（包括外国公司）参加，美国政府机构的代表以个人名义参加其活动。该学会是一个非政府、非盈利的机构，其经费来源于会费和标准资料销售收入，不接受政府的资助。

ANSI 作为标准制定的认可机构，其本身一般不制定标准。ANSI 的主要工作职责包括：①对标准制定者、技术顾问及合格评定体系资格进行认可；②批准和撤销美国国家标准；③保障国民和企业参与国际或国内的标准化活动；④保证美国自愿协同标准体系的完整性；⑤代表美国组织协调参与国际标准化活动。

该学会的标准绝大多数来自各专业标准，其下设的各行业技术管理委员会，负责审核各专业学会、协会团体制定的标准，将其中比较成熟且具有普遍意义的提升为国家标准。

ANSI 研究、评定、批准和发布了大量由标准制定组织制定的信息安全标准，包括信息安全管理指南、信息技术设备与安全、信息交换和国家安全应急准备、医疗保健信息安全框架指南等基础类和应用于各行业的信息安全标准。例如，《ANSI T1.2.11—1989 信息交换中远程通信优先服务 国家安全应急准备的表示法》、《ANSI/IEEE 1228—1994 软件安全方案标准》，《ANSI/IEEE 802.10g—1995 互通 LAN 安全标准》、《ANSI/TIA/EIA-102.AAAB—2002 数字地面移动无线电安全服务综述》等。该学会还研究采纳了大量国际标注化组织的信息安全标准，并发布为美国标准。例如，《ANSI/INCITS/ISO/IEC17799—2005 信息技术—安全技术—信息安全管理实施规范》、《ANSI/INCITS/ISO/IEC13335-1—2004 信息技术—安全技术—信息和通信技术安全管理》等。

二、美国国家标准技术研究院 NIST

美国国家标准技术研究院（NIST）隶属于美国商务部。根据 2002 年《联邦信息安全管理法案》（FISMA），美国国家标准和技术委员会负责为联邦政府编制相关标准、指南和其他文档，以帮助联邦政府通过管理成本有效的体系来保护其信息和信息系统。

NIST 最高领导层由院长、副院长和信息最高执行官三人组成。下设与信息技术有关的单位：Boulder 实验室、技术服务部、技术研发部、电子与电工实验室、信息技术实验室。其他部门和实验室还有 Baldrige 国家质量项目部、管理和财务部、生产发展合作部、生产工程实验室、化学科学技术实验室、材料科学工程实验室、物理实验室、建筑与防火研究室。组织结构如图 1.1 所示。

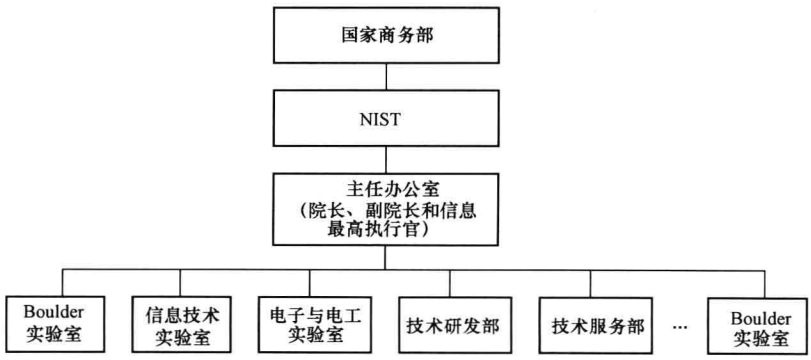

图 1.1 国家标准技术研究院组织结构

NIST 是美国信息安全技术标准领域最具影响的标准化机构，在美国信息安全管理工作中扮演着十分重要的角色。它制定的信息安全规范和标准很多，主要涉及访问控制和认证技术、评价和保障、密码、电子商务、一般计算机安全、网络安全、风险管理、电信、联邦信息处理等方面。早期最有影响的工作是制定了美国国家数据加密标准 DES，这项标准得到了广泛地应用，成为密码史上的一个里程碑。在密码方面公布了有关使用硬件正确实现数据加密、计算机安全和数据加密、计算机网络的密码公证系统、数据加密的维护测试、数字签名算法、完整性检验 HASH 函数、报文认证码 MAC、公开密钥密码等许多规范和指南。在系统安全方面公布了有关计算机安全系统脆弱性控制的审计和评价、测试计算机系统脆弱性的自动工具、SQL 数据库语言的安全性、防火墙、安全的数据网络、个人计算机系统安全管理、拨号安全、保护信息资源、计算机病毒及其威胁的管理、选择对抗病毒工具和技术、开放系统的安全等一系列规范和指南。

在电力工业信息安全方面，NIST 出版了 SP 800-82《工控系统安全指南》、SP 800-53《联邦信息系统推荐安全措施》和 NISTIR 7628 草案《智能电网网络安全策略与要求》。NIST 的专家还参与了美国国土安全部《控制系统安全建议目录》的撰写工作。

三、美国电力可靠性协会 NERC

1968 年，美国成立了电力可靠性协会（National Electric Reliability Council，NERC），1981 年由于加拿大和墨西哥的加入，改名为北美电力可靠性协会（North American Electric Reliability Council，NERC），NERC 的成立极大地推动了电力系统可靠性理论的研究及其在工程实际中的应用，同时也带动了世界各国电力可靠性管理工作的开展。

目前，北美电力可靠性协会理事会由 30 位成员组成，分别来自 9 个区域性的可靠性协会，及爱迪生电气研究所、加拿大的魁北克、新墨西哥电力公司以及独立的电力生产企业的代表等。NERC 总部设有 20 位专责人员及 10 多位秘书，组成日常办事机构即执行委员会。该委员会下设工程委员会和运行委员会。

NERC 有一个专门解决电力控制系统安全问题的工作组，于 2006 年 6 月发布了一系列“关键基础设施保护”（CIP）标准，包括关键网络资产识别、安全管理控制、人员与培训、电子安全周界、重大网络攻击下的物理安全、系统安全管理、事件报告和响应计划、重大网络攻击恢复流程等。为达到美国联邦能源管理委员会（FERC）的认证要求，NERC 于 2009 年对 CIP 各部分先后进行了更新，形成了 CIP 002-009 第二版。

1.1.3 主要国际信息安全标准

在信息安全领域，多个标准化组织从事信息安全标准化的制定工作。信息安全标准按照功能可以划分为技术标准、测评标准、管理标准和工程标准四类。

一、技术标准

1. 加密标准

密码学作为信息安全的基础，已经有几千年的历史。现代密码学中的许多加密算法都被定为标准，供军方和工业使用。

（1）数据加密标准 DES。数据加密标准（Data Encryption Standard, DES）作为 ANSI 的数据加密算法（Data Encryption Algorithm, DEA）和 ISO 的 DEA-1，成为一个世界范围

内的标准已经 20 多年了。1999 年，56 位密码的 DES 算法被证明可以在 23h 之内破解，目前 DES 算法被认为是不安全的。DES 的具体算法见第三章。尽管 DES 后来的变型算法都存在 DES 的理论缺陷，但是密钥很难计算出来，所以认为这些变型算法是安全的，如 3DES。

（2）高级加密标准 AES。高级加密标准（Advanced Encryption Standard，AES）是美国国家标准技术研究所 NIST 旨在取代 DES 的 21 世纪的加密标准。AES 也称 Rijndael 算法，由两位比利时密码学家发明，参与了 NIST（美国标准和技术委员会）1997 年组织的公开密码学竞赛，最终以优异的技术特性胜出成为加密标准。AES 的具体算法见第三章。

（3）安全散列算法 1 SHA-1。安全散列算法 1（Secure Hash Algorithm 1，SHA-1）由 NSA 开发，被 NIST 认可，并被标准化在 FIPS180-1 中。SHA-1 是一种消息摘要（Message Digest, MD）算法，以单向散列函数的思想为基础，按照 512 位的块大小来处理输入数据，生成一个 160 位的消息摘要。后来开发的 SHA-2，分别针对 256、384 和 512 位的散列值。

2. 安全通信协议

开发安全通信协议的目的是将数据位秘密地、未被篡改地从源端传送到目标端，将有害的数据位排除在门外。安全通信协议根据防护对象的不同，可以分为互联网通信安全协议、无线通信安全协议等；根据通信层次的不同，可以分为链路层通信安全协议、网络层通信安全协议、传输层通信安全协议和应用层通信安全协议。IETF 制定的 Internet 的通信安全标准应用较广，如 IPSec 和 TLS；IEEE 制定的无线通信安全协议应用较广，如 802.11i；3GPP 和 3GPP2 为 3G 移动通信系统定制了通信安全机制，IP 多媒体子系统（IP Multimedia Subsystem , IMS）的安全规范体系。

（1）IPSec。IPSec 在 IP 层提供安全服务，它使系统能按需选择安全协议，决定服务所使用的算法及放置需求服务所需密钥到相应位置。IPsec 用来保护一条或多条主机与主机间、安全网关与安全网关间、安全网关与主机间的路径。

IPSec 协议不是一个单独的协议，它给出了应用于 IP 层上网络数据安全的一整套体系结构，包括网络认证协议（Authentication Header，AH）、封装安全载荷协议（Encapsulating Security Payload，ESP）、密钥管理协议（Internet Key Exchange，IKE）和用于网络认证及加密的一些算法等。IPSec 规定了如何在对等层之间选择安全协议、确定安全算法和密钥交换，向上提供了访问控制、数据源认证、数据加密等网络安全服务。

（2）TLS。传输层安全（Transport Layer Security，TLS）协议，基于由 Netscape 发展的 SSL，在通信应用之间提供隐私和数据完整性。TLS 被网络浏览器广泛使用来为传递信用卡号和其他敏感信息提供安全连接（HTTPS）。尽管 SSL 被 IETF 标准化为 TLS，但是 IETF 对 SSL 所做的变化非常小，TLS 版本也被称为 SSL3.1 版。TLS 由两层组成：TLS 记录协议和 TLS 握手协议。在最低标准中，位于一些可靠传输协议（TCP） 顶层的是 TLS 记录协议。

（3）高级的无线局域网安全标准 IEEE 802.11i。为加强无线网络的安全性和不同厂家间无线安全技术的兼容性，2004 年 6 月 25 日，IEEE 工作组正式通过 802.11i 标准。IEEE 802.11i 把重点放在认证、密钥管理和数据传递的保密性三个领域。为改进认证，802.11i

要求使用认证服务器 AS（Authentication Server），并定义了一个更为健壮的认证协议。同时，AS 还起到密钥分发的作用。在保密性方面，802.11 i 提供了三种不同的加密机制，分别为 TKIP（Temporal Key Integrity Protocol），CCMP（Counter-Mode/CBC-MAC Protocol）和 WRAP（Wireless Robust Authenticated Protocol），以及认证协议 IEEE 802.1x。IEEE 802.11i 的操作过程：①在移动站点和 AP 之间的一次交换使双方在使用的安全能力集合上达成一致；②涉及 AP 和移动站点之间的一次交换提供了安全认证，AS 负责向 AP 分发密钥，AP 再依次向移动站点管理和分发密钥；③在移动站点和 AP 之间的数据采用加密来保护数据的传递。

IEEE 802.11i 为了保证兼容性，全面吸收其他现有的网络安全协议，如接入控制层引入现有 IEEE 802.1x 安全机制，上层管理层融入现有的 LEAP 及 RADIUS 服务器等功能。从硬件设备来看，AP 只涉及 WLAN 底层和接入控制层，涉及 802.11i 的数据加密协议和 IEEE 802.1x 的接入管理机制，其认证管理功能由认证服务器和远端数据库来完成。移动用户则包含了全部的三层，涉及了 802.11i 的底层数据加密协议，IEEE 802.1x 的接入管理机制和 IEEE 802.11x / EAP 认证管理机制。用户端和认证服务器都具有认证管理层的功能。

（4）IMS 安全规范体系。WCDMA、CDMA2000、TD-SCDMA 是 3G 移动通信的主流技术。WCDMA、TD-SCDMA 的安全规范由欧盟委员会主体的 3GPP（3G Partnership Project，3G 合作项目）制定，CDMA2000 的安全规范由以北美为首的 3GPP2 制定。

在 IMS 的安全体系中，3GPP 和 3GPP2 制定了一系列 IMS 网络安全标准。从 UE 到网络的各个实体（P-CSCF、S-CSCF、HSS）都涉及了接入和核心网两个部分的安全机制。对于接入部分，UE 与 P-CSCF 之间涉及接入安全与身份认证，其安全机制在 3GPPTS33.203《3G 安全：基于 IP 业务的服务的接入安全》中定义。IMS 以 SIP 和 HTTP 承载 AKA 安全机制的方式实现了 UE 与网络的双向认证功能；UE 与 P-CSCF 之间协商 SA（Security Association，安全联盟），通过 IPSec 提供了接入安全保护。IMS 在核心网中引入了网络域安全 NDS 的概念，对核心网中的所有 IP 业务流进行保护。网络域安全是由某个单独机构所管理的网络，在同一安全域内的网元具有相同的安全级别并享有特定的安全服务，主要通过为服务提供机密性、数据完整性、认证和防止重放攻击，以及通过应用在 IPSec 中的密码安全机制和协议安全机制来实现。网络域内部的实体和网络域之间都可以使用 IPSec 来提供安全保护。现有 IMS 安全标准体系在以下方面提供了较完善的解决方案：客户和网络的双向身份认证；UE 与 P-CSCF 之间的 SIP 信令消息的机密性保护；UE 与 P-CSCF 之间 SIP 信令的完整性保护；IMS 网络域的安全采用 hop-by-hop（逐跳）安全模式，对在网络实体之间的每个通信进行单独的保护；支持隐藏运营商网络拓扑的能力等。

二、测评标准

1. 评估准则 CC

目前，在信息安全评估领域，IT 安全性评估通用准则已成为评估信息系统及产品安全性的世界性通用准则。IT 安全性评估通用准则定义了评估信息技术产品和系统安全特

性的基础准则，提出了目前国际上公认的表述信息技术安全性的结构以及如何正确有效地实施这些功能的保证要求，是目前系统安全认证方面最权威的标准。GB 18336（等同ISO/IEC 15408—1999）《信息技术—安全技术—信息技术安全性评估准则》（简称 CC），作为评估信息技术产品和系统安全性的世界性通用准则，是信息技术安全性评估结果国际互认的基础。目前已有美国、加拿大、英国、法国、德国、荷兰等国加入此互认协定，日本、韩国、以色列等也正在积极准备加入此协定。

CC 是国际标准化组织为统一现有多种评估准则努力的结果，是在美国和欧洲等国分别自行推出并实践测评准则及标准的基础上，通过相互间的总结和互补发展起来的。

2. 可信计算机评估准则 TCSEC

可信计算机评估准则 TCSEC 由美国国家计算机安全中心（NCSC）开发，1985 年由美国国防部作为 DOD5200.28-STD 标准发布，由于其书皮的颜色为橙色，因此通常称为橘皮书。可信计算机评估准则，即橘皮书，是大家公认的第一个计算机系统的评估准则。它的出现，代表了信息安全保障领域从通信保密阶段进入了以关注计算机操作系统等为主的计算机安全（COMPUSEC）阶段。

可信计算机评估准则（TCSEC）提供了一种对产品的安全性划分等级的分类方法，方便用户根据自己的安全要求选择相应等级的安全产品，对产品厂商来说它提供了在产品中实施安全的规范。在 TCSEC 中，将安全级别从高到低分为 A、B、C、D 四类，级下再分 A1、B1、B2、B3、C1、C2、D 等 7 级。下面对 4 类 7 个安全等级作进一步介绍。

（1）D 类：最小保护。不符合 C1～A1 级安全要求标准的系统为 D 级，其安全水平最低。

（2）C 类：自主保护。C 类标准分 C1 和 C2 两个级别，要求用户定义访问控制，即用户能定义系统访问权限，并具有对主体责任和其初始动作审计的能力。

1）C1 级：自主安全保护。C1 级系统通过提供用户与数据的分离来满足无条件安全要求。它包括某种形式的可信控制，以便能在个体基础上执行访问限制，即外表上允许用户保护项目和保护私有数据，并阻止其他用户意外地读取或破坏他们的数据。C1 级环境是在同一敏感等级上处理数据的那些协同用户所要求的。大部分 UNIX 系统达到 C1 级标准要求。

2）C2 级：可控访问保护。在 C2 级系统中，实施一种比 C1 级细粒度更细的自主访问控制。可通过注册过程、与安全相关事件的审计以及资源隔离等措施，使用户对他们的活动分别负责。

UNIX 系统通常大部分达到 C2 级标准，Windows NT 也达到此级标准要求。

（3）B 类：强制保护。本类分为 B1、B2 和 B3 三个级别，它主要要求课题必须保留敏感标号，系统用它来加强访问控制保护。在本等级中，对于计算机系统中大多数数据结构都必须带有敏感标号；系统开发者要提供安全策略模型，根据此模型生成系统。同时系统开发者也要提供其技术规范说明并提供基准监控器概念已被实现的证据。

1）B1 级：标记安全保护。B1 级要求具有 C2 级的全部特征。另外，必须提出安全策略模型的非形式化说明、数据标号以及已命名主体对客体的强制访问控制。对输出的

信息必须有正确的标记能力；必须排除任何经测试而标识的缺陷。

UNIX 系统需做大量的工作（主要是文件编制）才能达到此级要求。某些 C2 级 UNIX 生产厂商也部分满足 B1 级标准要求，称为不完全 B1 级。

2）B2 级：结构化保护。在 B2 级中，系统是建立在对形式化安全策略模型清晰定义和提供文档基础之上的。该模型要求执行 B1 级所建立的自主和强制访问控制，并扩展到计算机系统的全部主题和客体。另外，还提出了隐蔽通道。系统必须是仔细地构成严格保护和非严格保护的单元。系统接口应定义恰当，而且系统设计和实现能使其经受比较彻底的测试和比较安全的检查。要加强鉴别机制，以支撑系统管理员和操作员功能的方式提供可信设施管理，而且要加强严格的配置管理控制。该系统有相对的抗渗透能力。

目前，达到 B2 级要求的商业操作系统很少。

3）B3 级：安全域保护。B3 级系统必须满足基准监控器的要求，以便它能仲裁所有主体向客体的访问。它必须是防篡改的，而且是小到足以提供分析和测试。为此，在系统设计及实现期间，要用有效的系统工程方法，使构造的系统能排除与安全策略实施无关的代码，从而使其复杂性达到最小。要支持安全管理员，要把审计机制扩展到用信号报知与安全有关的事件，并且要提供系统恢复过程。该系统有高度的抗渗透能力。

（4）A 类：验证保护。本等级的特征是使用形式化安全验证方法，以保证系统采用的强制和自主安全控制能有效保护该系统存储的保密或其他敏感信息。为了证明系统满足设计、开发和实现各方面的安全要求，需要扩展文件。

A1 级：验证设计。A1 级在功能上与 B3 级相同，不必增加任何关于策略或结构特性的要求。本等级的显著特点是用形式化顶层规范说明和验证技术来分析，以确保系统完全正确地实现。实际上，由于这种保证是开始于安全策略的形式化模型和设计形式化顶层规格说明，所以它是不断发展的。

为了配合 A1 级所要求的系统扩展设计和开发分析，需要更严格的配置管理，并建立把该级安全分析分配到现场的过程并要支持系统安全管理员。

三、管理标准

1. ISO/IEC 27000 系列信息安全管理体系

ISO/IEC 采用 27000 系列号码作为编码方案，将原先所有的信息安全管理标准进行综合并做进一步地开发，形成一整套包括 ISMS 要求、风险管理、度量和测量以及实施指南等在内的安全管理体系。ISO/IEC 27000 信息安全管理体系标准族正在不断地制定发布，并成功地被全球各业所采用。

（1）ISO/IEC 27001：2005。信息安全管理体系要求是该标准族的核心标准，是建立信息安全管理体系（ISMS）的一套规范，详细说明了建立、实施和维护信息安全管理体系的要求，其最终目的在于建立适合企业需要的信息安全管理体系（ISMS）。该标准已在世界范围内被公认为认证、合同及法规要求标准。

作为 ISO/IEC 27001 的补充，制定 ISO/IEC 27000 标准族中其他标准的目的是为按照 ISO/IEC 27001 的要求建立、实施和改进信息安全管理体系提供指南及支持。

（2）ISO/IEC 27002：2005。该标准是公认的信息安全管理行为规范。ISO 目前正在

对 ISO/IEC 27001 和 ISO/IEC 27002 进行五年期的评审修订，旨在实现管理体系标准的不断完善。

（3）ISO 27003: 2010。信息安全管理体系实施指南，其内容覆盖了信息安全管理体系的各个过程。它不仅给出了获得管理层批准的指南，也为有效实施 ISMS 提供了设计和策划的框架。这不仅有助于组织开发信息安全管理过程，也使相关方确信，组织的信息资产持续受控于组织的信息安全保护范围之内。

（4）ISO/IEC 27004：2009。信息安全管理测量与指标，该标准阐述信息安全管理的测量和指标，用于测量信息安全管理的实施效果。该标准将使企业的管理层能时刻跟踪信息安全管理体系的安全绩效。ISO/IEC 27004 包括了在检查 PDCA 过程模式时，有效性测量的内容、时机和方法，过程模式主要是指在监督和审查持续改进的过程阶段。

（5）ISO/IEC 27005：2008。信息安全风险管理。它给出了信息安全风险管理的指南，包括风险管理的原则、风险评估方法、风险处理和风险接受、风险的监视和评审等，以及给出了如何满足 ISMS 要求的更进一步的信息。

（6）ISO/IEC 27006：2007。信息安全管理体系审核指南。该标准为由认证资格的组织按照 ISO/IEC 27001 和 ISO/IEC 27001 审核带认证企业的 ISMS。ISO / IEC 27006 为认证机构理解 ISO 17021-1 中关于审核的条款和任何一个 ISMS 应如何符合 ISO / IEC 27001 的要求提供了指南。

（7）ISO/IEC 27007。信息安全管理体系审核指南和 ISO/IEC 27008 控制审核员指南目前正在开发之中。ISO/IEC 27007 是专门为 ISMS 的范围和复杂程度、风险管理、控制方法的选择和 ISMS 审核员的能力等方面提供审核指南的标准。ISO/IEC 27008 对 ISO/IEC 27001 附录 A 中规定的安全控制提出了技术要求。这两个标准已在 2011 年出版。

（8）行业标准。一系列 ISO/IEC 27001 行业应用新标准正在制订，它们引入了行业附加的特殊要求。目前的工作方案包括：

1）ISO/IEC 27010。行业间交流的信息安全管理，用于行业间的沟通。这个标准主要涉及那些国家基础设施的行业和组织的各类安全要求。这包括指令安全及控制应用措施，如监督控制和数据采集。

2）ISO/IEC 27011：2008。基于 ISO/IEC 27002 通信行业信息安全管理体系，适用于电信组织。该标准基于 ISO/IEC 27002，该标准已于 2008 年出版，电信标准号为 X.1051。

3）ISO/IEC 27013 ISO/IEC 20000-1 及 ISO/IEC 27001 一体化实施指南，该标准为那些希望将服务管理和信息安全管理体系的共性整合成为一体的机构提供指南。如，它们可将文件化体系、事故处理体系和安全服务提供、监督和审查程序整合起来。

4）ISO/IEC 27014 信息安全管理框架，该标准支持公司管理框架的信息安全。ISO/IEC 27001 是一个理想的信息安全框架，因为它包含三个关键管理要素，即风险管理、控制体系和审核职能。

5）ISO/IEC 27015 金融和保险服务业信息安全管理体系，该标准是 ISO/IEC 27001 标准在金融和保险业的特殊运用。