YD

中华人民共和国通信行业标准

YD/T 1728-2008

电信网和互联网安全防护管理指南

Security Protection Management Guide for
Telecom Network and Internet

2008-01-14 发布　　2008-01-14 实施

中华人民共和国信息产业部　发布

目　次

前　言

本标准是“电信网和互联网安全防护体系”系列标准之一。该系列标准的结构及名称如下：

1. YD/T 1728-2008　电信网和互联网安全防护管理指南；
2. YD/T 1729-2008　电信网和互联网安全等级保护实施指南；
3. YD/T 1730-2008　电信网和互联网安全风险评估实施指南；
4. YD/T 1731-2008　电信网和互联网灾难备份及恢复实施指南；
5. YD/T 1732-2008　固定通信网安全防护要求；
6. YD/T 1733-2008　固定通信网安全防护检测要求；
7. YD/T 1734-2008　移动通信网安全防护要求；
8. YD/T 1735-2008　移动通信网安全防护检测要求；
9. YD/T 1736-2008　互联网安全防护要求；
10. YD/T 1737-2008　互联网安全防护检测要求；
11. YD/T 1738-2008　增值业务网——消息网安全防护要求；
12. YD/T 1739-2008　增值业务网——消息网安全防护检测要求；
13. YD/T 1740-2008　增值业务网——智能网安全防护要求；
14. YD/T 1741-2008　增值业务网——智能网安全防护检测要求；
15. YD/T 1742-2008　接入网安全防护要求；
16. YD/T 1743-2008　接入网安全防护检测要求；
17. YD/T 1744-2008　传送网安全防护要求；
18. YD/T 1745-2008　传送网安全防护检测要求；
19. YD/T 1746-2008　IP承载网安全防护要求；
20. YD/T 1747-2008　IP承载网安全防护检测要求；
21. YD/T 1748-2008　信令网安全防护要求；
22. YD/T 1749-2008　信令网安全防护检测要求；
23. YD/T 1750-2008　同步网安全防护要求；
24. YD/T 1751-2008　同步网安全防护检测要求；
25. YD/T 1752-2008　支撑网安全防护要求；
26. YD/T 1753-2008　支撑网安全防护检测要求；
27. YD/T 1754-2008　电信网和互联网物理环境安全等级保护要求；
28. YD/T 1755-2008　电信网和互联网物理环境安全等级保护检测要求；
29. YD/T 1756-2008　电信网和互联网管理安全等级保护要求；
30. YD/T 1757-2008　电信网和互联网管理安全等级保护检测要求；
31. YD/T 1758-2008　非核心生产单元安全防护要求；
32. YD/T 1759-2008　非核心生产单元安全防护检测要求。

随着电信网和互联网的发展，将不断补充和完善电信网和互联网安全防护体系的相关标准。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：信息产业部电信研究院、中国电信集团公司、中国移动通信集团公司、中国网络通信集团公司、中国联合通信有限公司、中国铁通集团有限公司

本标准主要起草人：田慧蓉、杨　洋、王新峰、魏丽红、殷　琪、徐　楠、严　萍

电信网和互联网安全防护管理指南

1 范围

本标准对电信网和互联网安全防护的定义、目标、原则进行了描述和规范。同时，对电信网和互联网安全防护体系、安全防护体系三部分工作及其关系进行了说明。

本标准适用于电信网和互联网的安全防护工作。

本标准涉及的电信网和互联网不包括专用网，仅指公众电信网和公众互联网。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为指导性技术文件的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 5271.8-2001 信息技术 词汇 第8部分：安全

3 术语和定义

GB/T 5271.8-2001确立的术语和定义以及下列术语和定义适用于本标准。

3.1

电信网 Telecom Network

利用有线和/或无线的电磁、光电系统，进行文字、声音、数据、图像或其他任何媒体的信息传递的网络，包括固定通信网、移动通信网等。

3.2

互联网 Internet

泛指广域网、局域网及终端（包括计算机、手机等）通过交换机、路由器、网络接入设备等基于一定的通信协议连接形成的，功能和逻辑上的大型网络。

3.3

电信网和互联网安全防护体系 Security Protection Architecture of Telecom Network and Internet

电信网和互联网的安全等级保护、安全风险评估、灾难备份及恢复三项工作互为依托、互为补充、相互配合，共同构成了电信网和互联网安全防护体系。

3.4

电信网和互联网安全等级 Security Classification of Telecom Network and Internet

电信网和互联网及相关系统重要程度的表征。重要程度从电信网和互联网及相关系统受到破坏后，对国家安全、社会秩序、经济运行、公共利益、网络和业务运营商造成的损害来衡量。

3.5

电信网和互联网安全等级保护 Classified Security Protection of Telecom Network and Internet

指对电信网和互联网及相关系统分等级实施安全保护。

3.6

电信网和互联网安全风险 Security risk of Telecom Network and Internet

人为或自然的威胁可能利用电信网和互联网及相关系统存在的脆弱性导致安全事件的发生及其对组织造成的影响。

3.7

电信网和互联网安全风险评估　Security Risk Assessment of Telecom Network and Internet

指运用科学的方法和手段，系统地分析电信网和互联网及相关系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生，可能造成的危害程度，提出有针对性的抵御威胁的防护对策和安全措施，防范和化解电信网和互联网及相关系统安全风险，将风险控制在可接受的水平，为最大限度地保障电信网和互联网及相关系统的安全提供科学依据。

3.8

电信网和互联网灾难　Disaster of Telecom Network and Internet

由于各种原因，造成电信网和互联网及相关系统故障或瘫痪，使电信网和互联网及相关系统支持的业务功能停顿或服务水平不可接受、达到特定的时间的突发性事件。

3.9

电信网和互联网灾难备份　Backup for Disaster Recovery of Telecom Network and Internet

为了电信网和互联网及相关系统灾难恢复而对相关网络要素进行备份的过程。

3.10

电信网和互联网灾难恢复　Disaster Recovery of Telecom Network and Internet

为了将电信网和互联网及相关系统从灾难造成的故障或瘫痪状态恢复到正常运行状态或部分正常运行状态、并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。

4　目标和原则

电信网和互联网安全防护工作的目标就是要加强电信网和互联网的安全防护能力，确保网络的安全性和可靠性，尽可能实现对电信网和互联网安全状况的实时掌控，保证电信网和互联网能够完成其使命。为了实现该目标，网络和业务运营商、设备制造商要充分考虑电信网和互联网不同等级的安全要求，从环境因素以及人为因素分析电信网和互联网面临的威胁，从技术和管理两个方面分析电信网和互联网存在的脆弱性，充分考虑现有安全措施，分析电信网和互联网现存风险，平衡效益与成本，制定灾难备份及恢复计划，将电信网和互联网的安全控制在可接受的水平。

电信网和互联网安全防护工作要在适度安全原则的指导下，采用自主保护和重点保护方法，在安全防护工作安排部署过程中遵循标准性、可控性、完备性、最小影响和保密原则，实现同步建设、统筹兼顾、经济实用和循序渐进地进行安全防护工作。

——适度安全原则：安全防护工作的根本性原则。安全防护工作应根据电信网和互联网的安全等级，平衡效益与成本，采取适度的安全技术和管理措施。

——标准性原则：安全防护工作开展的指导性原则。指电信网和互联网安全防护工作的开展应遵循相关的国家或行业标准。

——可控性原则：指电信网和互联网安全防护工作的可控性，包括以下三个方面。

- 人员可控性：相关的安全防护工作人员应具备可靠的政治素质、职业素质和专业素质。相关安全防护工作的检测机构应具有主管部门授权的电信网和互联网安全防护检测服务资质。
- 工具可控性：要充分了解安全防护工作中所使用的技术工具，并进行一些实验，确保这些技术工

具能被正确地使用。

- 项目过程可控性：要对整个安全防护项目进行科学的项目管理，实现项目过程的可控性。

——完备性原则：安全防护工作要覆盖电信网和互联网的安全范围。

——最小影响原则：从项目管理层面和技术管理层面，将安全防护工作对电信网和互联网正常运行的可能影响降低到最低限度。

——保密性原则：相关安全防护工作人员应签署协议，承诺对所进行的安全防护工作保密，确保不泄露电信网和互联网及安全防护工作的重要和敏感信息。

5 安全防护体系

电信网和互联网安全防护范畴包括基础电信运营企业运营的传输、承载各类电信业务的公共电信网（含公共互联网）及其组成部分，支撑和管理公共电信网及电信业务的业务单元和控制单元以及企业办公系统（含文件管理系统、员工邮件系统、决策支持系统、人事管理系统等）、客服呼叫中心、企业门户网站等非核心生产单元。此外，电信网络安全防护工作的范围还包括经营性互联网信息服务单位、移动信息服务单位、互联网接入服务单位、互联网数据中心、互联网域名服务机构等单位运营的网络或信息系统。

根据电信网和互联网安全防护范畴，建立的电信网和互联网安全防护体系如图1所示。整个体系分为三层，第一层为整个安全防护体系的总体指导性规范，明确了对电信网和互联网安全防护的定义、目标、原则，并说明了安全防护体系的组成。

第二层从宏观的角度明确了如何进行安全防护工作，规范了安全防护体系中安全等级保护、安全风险评估、灾难备份及恢复三部分工作的原则、流程、方法、步骤等。

第三层具体规定了电信网和互联网安全防护工作的要求，即安全防护要求和安全防护检测要求。

根据电信网和互联网全程全网的特点，电信网和互联网的安全防护工作可从固定通信网、移动通信网、互联网、增值业务网、非核心生产单元来开展。其中，互联网包括经营性互联网信息服务单位、互联网接入服务单位、互联网数据中心、互联网域名服务机构等单位运营的网络或信息系统。增值业务网包括消息网、智能网等业务平台以及业务管理平台。

对固定通信网、移动通信网、互联网实施安全防护，应分别从构成上述网络的不同电信网和互联网相关系统入手。电信网和互联网相关系统包括接入网、传送网、IP承载网、信令网、同步网、支撑网等。其中，接入网包括各种有线、无线和卫星接入网等，传送网包括光缆、波分、SDH、卫星等，而支撑网则包括业务支撑和网管系统。

安全防护要求明确了电信网和互联网及相关系统需要落实的安全管理和技术措施，涵盖了安全等级保护、安全风险评估、灾难备份及恢复等三部分内容，其中安全等级保护工作需要落实的物理环境和管理的安全等级保护要求被单独提出作为电信网和互联网及相关系统的通用安全等级保护要求。

安全防护检测要求与安全防护要求相对应，提供了对电信网和互联网安全防护工作进行检测的方法，从而确认网络和业务运营商、设备制造商在安全防护工作实施过程中是否满足了相关安全防护要求。

随着电信网和互联网的发展，随着安全防护体系的进一步完善，第三层的内容将进一步补充完善。

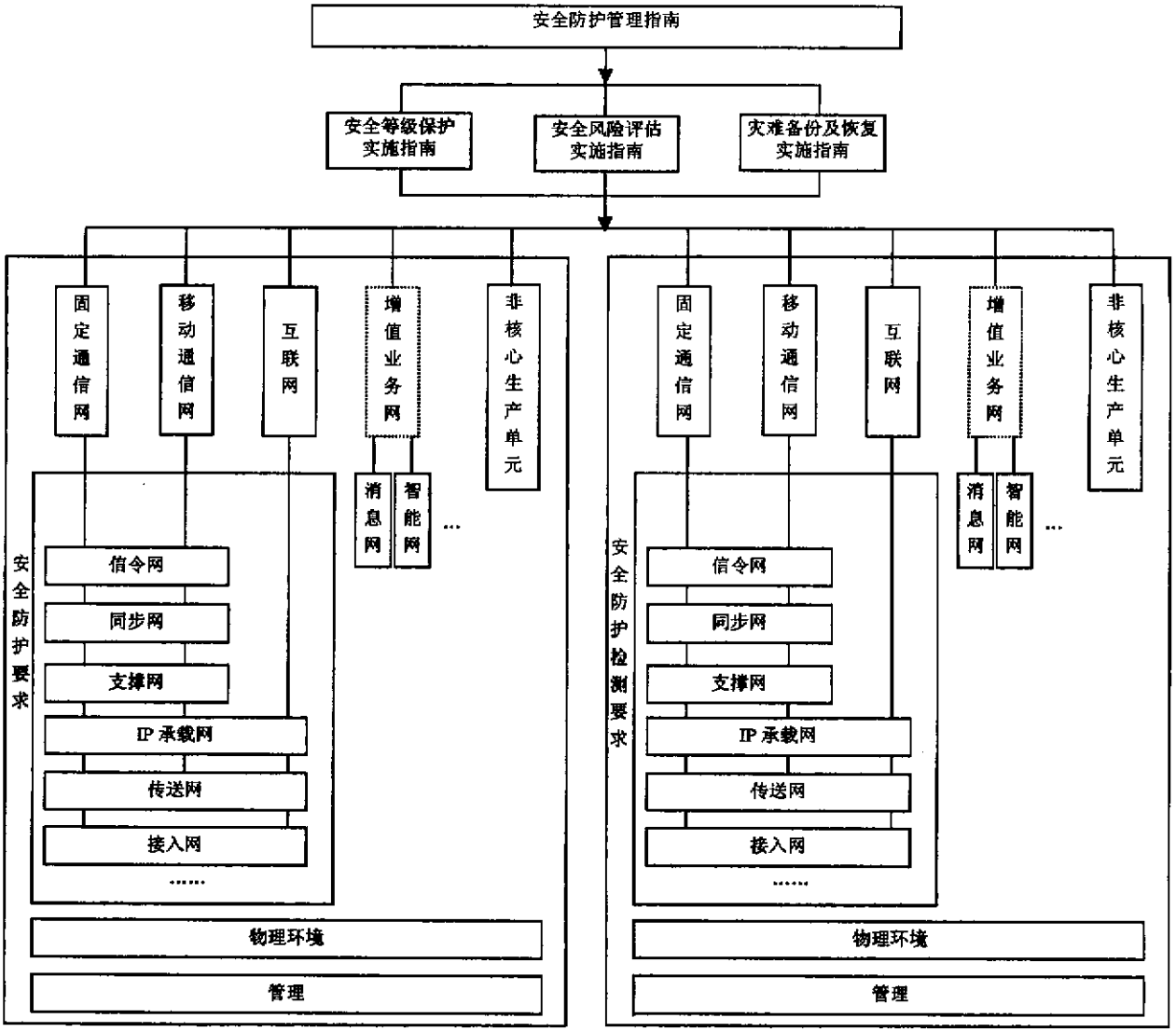

图1 电信网和互联网安全防护体系

6 安全等级保护

电信网和互联网安全等级保护工作贯穿于电信网和互联网生命周期的各个阶段，是一个不断循环和不断提高的过程。首先，根据电信网和互联网及相关系统受到破坏后，对国家安全、社会秩序、经济运行、公共利益、网络和业务运营商造成的损害程度来确定安全等级。通过进一步分析电信网和互联网及相关系统的安全保护现状与安全等级保护要求之间的差距，确定安全需求，设计合理的、满足安全等级保护要求的总体安全方案，制定出安全建设规划。并进一步将其落实到电信网和互联网及相关系统中，形成安全技术和管理体系。在电信网和互联网安全运维阶段，根据安全等级保护的需要对安全技术和管理体系不断调整和持续改进，确保电信网和互联网及相关系统满足相应等级的安全要求；在安全资产终止阶段对信息、设备、介质进行终止处理时，防止敏感信息的泄露，保障电信网和互联网及相关系统的安全。安全等级保护工作的实施过程如图2所示。

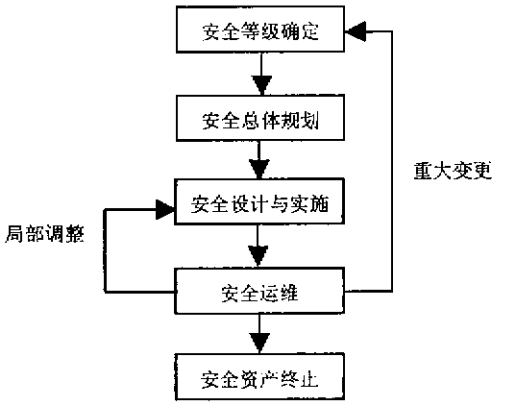

图2 安全等级保护实施的基本过程

7 安全风险评估

电信网和互联网安全风险评估应贯穿于电信网和互联网生命周期的各阶段中，在生命周期不同阶段的风险评估原则和方法是一致的。在电信网和互联网的安全风险评估工作中，应首先进行相关工作的准备，通过安全风险分析计算电信网和互联网及相关系统的风险值，进而确定其风险等级和风险防范措施。安全风险分析中要涉及资产、威胁、脆弱性等基本要素，每个要素有各自的属性。资产的属性是资产价值；威胁的属性可以是威胁主体、影响对象、出现频率、动机等；脆弱性的属性是资产弱点的严重程度等。安全风险评估的实施流程如图3所示。

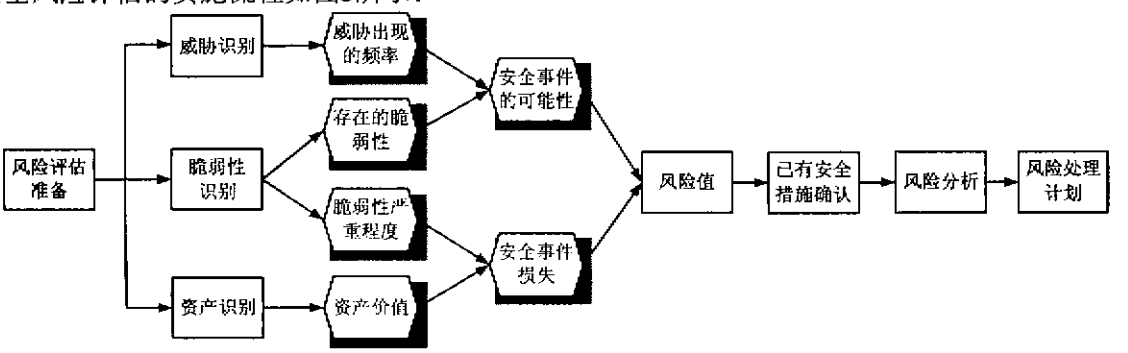

图3 安全风险评估实施的基本过程

8 灾难备份及恢复

电信网和互联网灾难备份及恢复工作利用技术、管理手段以及相关资源，确保已有的电信网和互联网在灾难发生后，在确定的时间内可以恢复和继续运行。灾难备份及恢复工作需要防范包括地震、水灾等自然灾难以及火灾、战争、恐怖袭击、网络攻击、设备系统故障、人为破坏等无法预料的突发事件。如图4所示，灾难备份及恢复工作应根据安全等级保护确定的安全等级以及安全风险分析的相关结果进行需求分析，制定、实现相应的灾难备份及恢复策略，并构建灾难恢复预案，这是一个循环改进的过程。

针对电信网和互联网的不同网络、不同重要级别的业务，灾难备份及恢复所要达到的目标是不同的。例如，在电信网和互联网中，对于普通语音业务，可以要求网络和业务运营商通过灾难备份及恢复工作，保证在灾难发生后单一地区的灾难不影响灾难发生地理范围以外地区的语音业务，并且发生灾难的地区的语音业务能够通过有效灾难恢复计划的实施，在一定时间范围（指标应与灾难级别对应）内恢复通信。

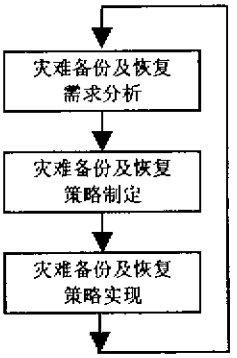

图4 灾难备份及恢复实施的基本过程

9 安全等级保护、安全风险评估、灾难备份及恢复三者之间的关系

电信网和互联网安全防护体系中的安全等级保护、安全风险评估、灾难备份及恢复三者之间密切相关、互相渗透、互为补充。电信网和互联网安全防护应将安全等级保护、安全风险评估、灾难备份及恢复工作有机结合，加强相关工作之间的整合和衔接，保证电信网络安全防护工作的整体性、统一性和协调性。电信网络安全防护工作应按照根据被保护对象的重要性进行分等级保护的思想，通过安全风险评估的方法正确认识被保护对象存在的脆弱性和面临的威胁，进而制定、落实和改进与安全保护等级和风险大小相适应的一系列管理、技术、灾难备份等安全等级保护措施，最终达到提高电信网络安全保护能力和水平的目的。

在开展安全等级保护工作时，要充分应用安全风险评估的方法，认识、分析不同类型的网络和业务存在的脆弱性和面临的威胁，进而制定和落实与被保护对象的类型、脆弱性和威胁相适应的基本安全保护措施要求，提高安全等级保护工作的针对性和适用性。在开展安全风险评估工作时，在分析被保护对象综合风险和制定改进方案的过程中，要始终与被保护对象的安全保护等级相结合，合理确定被评估对象的可接受风险和制定确实必要的整改措施，避免无限度地改进提高。在开展灾难备份及恢复工作时，要结合被备份对象的安全保护等级和面临的威胁，制定相适应的备份措施，并将有关备份的要求体现在安全等级保护的要求中进行落实。

电信网和互联网安全等级保护、安全风险评估和灾难备份及恢复工作应随着电信网和互联网的发展变化而动态调整，适应国家对电信网和互联网的安全要求。

参 考 文 献

1. YD/T 1729-2008　　电信网和互联网安全等级保护实施指南
2. YD/T 1730-2008　　电信网和互联网安全风险评估实施指南
3. YD/T 1731-2008　　电信网和互联网灾难备份及恢复实施指南