YD

中华人民共和国通信行业标准

YD/T 1736-2008

互联网安全防护要求

Security Protection Requirements for 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。

本标准与YD/T 1737-2008《互联网安全防护检测要求》配套使用。

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

本标准主要起草人：杨　洋、田慧蓉、赵　阳、刘　楠、李金玉、杜之亭、张云勇

互联网安全防护要求

1 范围

本标准规定了互联网业务及应用系统在安全等级保护、安全风险评估、灾难备份及恢复等方面的安全防护要求。

本标准适用于互联网业务及应用系统。

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本标准的条款。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。

YD/T 1729-2008 电信网和互联网安全等级保护实施指南

YD/T 1731-2008 电信网和互联网灾难备份及恢复实施指南

YD/T 1742-2008 接入网安全防护要求

YD/T 1744-2008 传送网安全防护要求

YD/T 1746-2008 IP 承载网安全防护要求

YD/T 1754-2008 电信网和互联网物理环境安全等级保护要求

YD/T 1756-2008 电信网和互联网管理安全等级保护要求

YD/T 1658-2007 宽带网络接入服务器安全技术要求

YD/T 1045-2000 网络接入服务器技术规范

YD/T 1311-2004 防范互联网垃圾电子邮件技术要求

YD/T 126-2005 增值电信业务网络信息安全保障基本要求

3 术语和定义

下列术语和定义适用于本标准。

3.1

互联网相关系统 Systems of Internet

组成互联网的相关系统，包括接入网、传送网、IP承载网等，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。

3.2

互联网安全等级 Security Classification of Internet

互联网及相关系统重要程度的表征。重要程度从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。

3.3

互联网安全等级保护 Classified Security Protection of Internet

对互联网及相关系统分等级实施安全保护。

3.4

组织 Organization

组织是由互联网及相关系统中不同作用的个体为实施共同的业务目标而建立的结构，组织的特性在于为完成目标而分工、合作；一个单位是一个组织，某个业务部门也可以是一个组织。

3.5

互联网安全风险 Security Risk of Internet

人为或自然的威胁可能利用互联网及相关系统中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。

3.6

互联网安全风险评估 Security Risk Assessment of Internet

指运用科学的方法和手段，系统地分析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，为最大限度地保障互联网及相关系统的安全提供科学依据。

3.7

互联网资产 Asset of Internet

互联网及相关系统中具有价值的资源，是安全防护体系保护的对象。互联网及相关系统中的资产可能以多种形式存在，无形的、有形的、硬件、软件，包括物理布局、通信设备、物理线路、数据、软件、文档、规程、业务、人员、管理等各种类型的资源，如IP承载网中的路由器、传送网的网络布局。

3.8

互联网资产价值 Asset Value of Internet

互联网及相关系统中资产的重要程度或敏感程度。资产价值是资产的属性，也是进行资产识别的主要内容。

3.9

互联网威胁 Threat of Internet

可能导致对互联网及相关系统产生危害的不希望事故潜在起因，它可能是人为的，也可能是非人为的；可能是无意失误，也可能是恶意攻击。

3.10

互联网脆弱性 Vulnerability of Internet

互联网及相关系统资产中存在的弱点、缺陷与不足，不直接对互联网资产造成危害，但可能被互联网威胁所利用从而危害互联网资产的安全。

3.11

互联网灾难 Disaster of Internet

由于各种原因，造成互联网及相关系统故障或瘫痪，使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。

3.12

互联网灾难备份 Backup for Disaster Recovery of Internet

为了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。

3.13

互联网灾难恢复 Disaster Recovery of Internet

为了将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 缩略语

下列缩略语适用于本标准。

DoS	Denial of Service	拒绝服务
DNS	Domain Name System	域名系统
FTP	File Transfer Protocol	文件传输协议
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
VPN	Virtual Private Network	虚拟专用网

5 互联网安全防护概述

5.1 互联网安全防护范围

互联网泛指广域网、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。互联网安全防护范围包括互联网业务及应用系统以及互联网相关系统。

目前运营的互联网业务包括互联网域名服务、互联网数据中心、互联网接入服务、互联网信息服务、在线数据处理与交易处理、移动互联网信息服务等。主流的互联网信息服务包括 Web 浏览、电子邮件、FTP、公众信息发布等，主流的移动互联网信息服务包括信息浏览、电子邮件、下载业务等。这些业务及应用涉及 DNS 服务器、域名注册/交易服务器、宽带网络接入服务器、网络接入服务器、Web 服务器、电子邮件服务器、FTP 服务器、公众信息发布服务器、在线数据处理与交易处理服务器、数据库服务器等互联网业务及应用系统的相关服务器以及用户端网络设备。

互联网相关系统组成如图 1 所示。

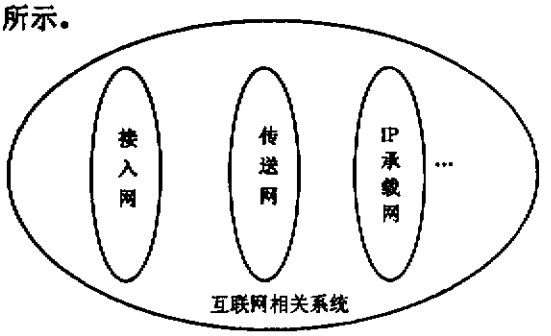

图 1 互联网相关系统

应对互联网业务及应用系统以及各相关系统分别实施安全等级保护、安全风险评估、灾难备份及恢复等工作，在此基础上充分考虑互联网业务及应用系统以及各相关系统之间的关系和相互影响，实现对互联网的整体安全防护。

本标准主要对互联网业务及应用系统提出安全防护要求，随着互联网业务及应用的发展，本标准将不断补充完善。互联网相关系统中接入网安全防护的具体要求参见 YD/T 1742-2008《接入网安全防护要求》，传送网安全防护的具体要求参见 YD/T 1744-2008《传送网安全防护要求》，IP 承载网安全防护的具体要求参见 YD/T 1746-2008《IP 承载网安全防护要求》。

5.2 互联网安全防护内容

根据电信网和互联网安全防护体系的要求，将互联网安全防护内容分为安全等级保护、安全风险评估、灾难备份及恢复等3个部分：

——互联网安全等级保护

主要包括定级对象和安全等级确定、业务及应用安全、设备安全、物理环境安全、管理安全等。

——互联网安全风险评估

主要包括互联网资产识别、脆弱性识别、威胁识别、已有安全措施确认、安全风险分析、安全风险评估文件处理等，本标准仅对互联网业务及应用系统进行资产分析、脆弱性分析、威胁分析，在互联网业务及应用系统安全风险评估过程中对资产、脆弱性、威胁的赋值方法及资产价值、风险值的计算方法参见YD/T 1730-2008《电信网和互联网安全风险评估实施指南》。

——互联网灾难备份及恢复

主要包括灾难备份及恢复等级确定、针对灾难备份及恢复各资源要素的具体实施等。

6 互联网定级对象和安全等级确定

我国具有管辖权的互联网业务及应用系统的定级对象为各个互联网业务及应用系统。

网络和业务运营商应根据YD/T 1729-2008《电信网和互联网安全等级保护实施指南》附录A中确定网络安全等级的方法对互联网业务及应用系统定级。针对业务及应用系统，可根据相应的社会影响力、所提供服务的重要性、服务用户数的大小进行定级，权重α、β、γ可根据具体业务及应用的情况进行调节。

7 互联网资产、脆弱性、威胁分析

7.1 资产分析

互联网业务及应用系统的资产至少应包括：设备硬件、设备软件、重要数据、提供的应用、文档、人员等，如表1所示。

表1 资产列表

分 类	主要资产
设备硬件	和各种互联网业务及应用的正常提供相关的服务器，包括DNS服务器、域名注册/交易服务器、宽带网络接入服务器、网络接入服务器、Web服务器、电子邮件服务器、FTP服务器、公众信息发布服务器、在线数据处理与交易处理服务器、数据库服务器等； 和各种互联网业务及应用的正常提供相关的用户端网络设备，包括路由器、交换机、网管系统设备等； 和各种互联网业务及应用正常提供相关的用户端网络链路； 相关服务器和用户端网络设备的操作维护系统； 相应的数据存储和备份介质等
设备软件	相关服务器和用户端网络设备的操作系统和应用软件等； 相关服务器和用户端网络设备的操作维护系统软件
重要数据	保证互联网业务和应用正常提供的重要数据，包括业务数据、系统配置数据、管理员操作维护记录、用户信息等
业务及应用	互联网可提供的各种业务及应用，包括互联网域名服务、互联网数据中心、互联网接入服务、互联网信息服务、在线数据处理与交易处理、移动互联网信息服务等
文档	纸质以及保存在存储介质中的各种文件，如设计文档、技术要求、管理规定（机构设置、管理制度、人员管理办法）、工作计划、技术或财务报告、用户手册等
人员	如相关服务器和用户端网络设备维护人员、系统开发人员、数据备份人员等

7.2 脆弱性分析

互联网业务及应用系统的脆弱性可以从技术脆弱性和管理脆弱性2个方面考虑。脆弱性识别对象应以资产为核心。表2给出了主要的脆弱性识别内容。

表2 脆弱性分析表

类 型	对 象	存在的主要脆弱性
技术脆弱性	业务及应用	相关服务器未进行合理备份，重要数据未及时进行备份。 相关业务/应用协议存在漏洞，相关服务器的应用代码存在漏洞、后门；相关服务器存在过多不必要的开放端口。 相关服务器配置不合理，访问控制策略存在漏洞。 相关服务器的日志功能没有启用或不够详细。 用户端网络规划和拓扑、设备部署、链路部署、资源配置、网络保护和恢复能力、安全技术措施和策略等方面的缺陷
	设备	相关服务器和用户端网络设备存在硬件隐患或质量问题； 相关服务器和用户端网络设备的操作系统存在安全隐患； 相关口令不够复杂、合理或没有经常更新； 重要部件未配置主备用保护； 相关服务器和用户端网络设备超过使用年限或核心部件老化； 相关服务器和用户端网络设备发生故障后未及时告警
	物理环境	机房场地选择不合理； 防火、供配电、防静电、接地与防雷、电磁防护、温湿度控制不符合规范； 通信线路、相关服务器和用户端网络设备的保护不符合规范
管理脆弱性		安全管理机构方面：岗位设置不合理（如人员配置过少、职责不清）、授权和审批程序简化、沟通和合作未执行、审核和检查未执行等； 安全管理制度方面：管理制度不完善、制度评审和修订不及时等； 人员安全管理方面：人员录用不符合程序、人员离岗未办理安全手续、人员未进行安全培训、对于第三方人员未进行限制访问等； 建设管理方面：安全方案不完善、软件开发不符合程序、工程实施未进行安全验收或验收不严格等； 运维管理方面：物理环境管理措施简单、存储介质使用不受限、设备没有定期维护、厂家支持力度不够、关键性能指标没有定期监控、无恶意代码防范措施、无数据备份和恢复策略、访问控制不严格、操作管理不规范等，应急保障措施不到位，灾难恢复预案不完善

7.3 威胁分析

互联网业务及应用系统面临的威胁可分为技术威胁、环境威胁和人为威胁。环境威胁包括自然界不可抗的威胁和其他物理威胁。根据威胁的动机，人为威胁又可分为恶意和非恶意两种。表3列举了互联网主要面临的威胁。

表3 威胁来源列表

来 源		主要威胁描述
技术威胁		相关服务器和用户端网络设备使用时间过长或质量问题等导致硬件故障； 用户端网络链路发生故障； 相关服务器和用户端网络设备的操作系统软件、应用软件运行故障； 相关服务器和用户端网络设备数据丢失或系统运行中断； 存储介质老化或质量问题等导致不可用
环境威胁	物理环境	断电、静电、灰尘、潮湿、温湿度异常、电磁干扰等； 意外事故或通信线路方面的故障
	自然灾害	鼠蚁虫害、洪灾、火灾、泥石流、山体滑坡、地震、台风、雷击、闪电
人为威胁	恶意人员	不满的或有预谋的内部人员滥用权限进行恶意破坏； 攻击者利用非法手段进入机房内部盗窃、破坏等，攻击者非法物理访问相关服务器、用户端网络设备、存储介质等； 攻击者利用网络协议、操作系统、应用系统漏洞，越权访问相关服务器和用户端网络设备的文件、数据或其他资源； 攻击者利用各种工具获取相关服务器和用户端网络设备身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问应用系统，或非法使用相关文件和数据； 攻击者利用应用系统扩散病毒、蠕虫、木马、垃圾电子邮件，利用相关攻击工具恶意消耗应用系统资源，导致系统能力下降或瘫痪、无法正常提供应用服务； 攻击者截获数据，进行篡改、插入，并重发，造成数据的完整性、真实性丧失
	无恶意人员	内部人员由于缺乏责任心或者无作为而应该执行而没有执行相应的操作、或无意地执行了错误或危险的操作导致安全事件； 内部人员没有遵循规章制度和操作流程而导致故障或信息损坏；内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致故障或攻击； 安全管理制度不完善、落实不到位造成安全管理不规范或者管理混乱导致安全事件

8 互联网安全等级保护要求

8.1 第1级要求

不作要求。

8.2 第2级要求

8.2.1 互联网业务及应用安全要求

8.2.1.1 通用安全要求

a） 应保护用户隐私，不泄漏用户相关信息；

b） DNS服务器、域名注册/交易服务器、宽带网络接入服务器、网络接入服务器、Web服务器、电子邮件服务器、FTP服务器、公众信息发布服务器、在线数据处理与交易处理服务器、数据库服务器等相关服务器应使用防火墙和防病毒等软件，应具备一定的容错、防病毒传播、防恶意软件、防DoS攻击、防黑客攻击及防范其他来自内部和外部各种常见攻击的能力；

c） 相关服务器应定期更新各种软件、系统补丁，定期检查相关服务器安全状况，并做相应检查记录；

d） 应通过IP地址、用户名、子网域名等方式对相关服务器的管理和各种操作进行控制，并保留相应的管理和操作记录，相关服务器应设置必要的读写权限和访问控制策略，应给予用户执行日常任务所

必需的最低等级的访问许可权，相应口令应足够复杂，相应口令应经常更换，应尽可能减少相关服务器的共享和开放端口；

e） 在向用户提供业务/应用时应保证相关系统之间传送信息的真实性和完整性，相关系统之间的认证、授权、安全协议及安全算法应满足相应标准的要求；

f） 互联网应用系统的用户端网络安全具体要求参见YD/T 1746-2008《IP承载网安全防护要求》第2级要求。

8.2.1.2 互联网域名服务安全要求

a） 提供域名注册服务的机构，应对注册的域名进行审查，杜绝不良域名的出现；

b） 应确保重要数据例如域名信息的安全性，防止被篡改和破坏；

c） 针对互联网域名解析服务，在排除外力因素（非本企业可控制的因素）的情况下，DNS服务器组的可用性应≥99.99%；

d） 针对不同的服务，应保存相应的服务记录，并保留一定期限，以便需要时能够查询相关信息，并避免相关数据和信息被篡改和破坏。

8.2.1.3 互联网数据中心安全要求

a） 应保护客户相关资产的安全性，包括硬件、软件、数据以及应用等；

b） 对托管/代维的服务器，应按照托管/代维的要求对网络带宽、电力系统、环境等进行管理；

c） 对代维的服务器，应按照代维的要求对服务器进行维护管理，保证服务器的正常运行；

d） 应按照客户的要求，记录对相关服务器的操作访问等日志，并保留一定期限，以便需要时能够查询相关信息，并避免相关数据和信息被篡改和破坏。

8.2.1.4 互联网接入服务安全要求

参见YDN 126-2005《增值电信业务网络信息安全保障基本要求》附录A。

8.2.1.5 互联网信息服务安全要求

8.2.1.5.1 Web 浏览安全

a） 应保护业务相关信息的安全，避免相关数据和页面被篡改和破坏；

b） 应禁止不必要的内嵌网络服务，应禁止在用户端自动安装恶意软件，应监控用户下载的软件是否含有病毒，并自动采取相应处理措施；

c） 对外提供Web浏览服务的平台不应向公众发布有害信息；

d） 应记录向公众发布的信息内容及其发布时间、互联网地址或者域名等，并保存60日（业务日志的内容和保留期限参照《互联网信息服务管理办法》，如果该法规修订，则本标准应作相应改动），以便需要时能够查询相关信息，应避免相关数据和信息被篡改和破坏；

e） 应对用户访问Web服务器的操作进行日志记录，以便需要时能够查询相关信息，应避免相关数据和信息被篡改和破坏。

8.2.1.5.2 电子邮件安全

a） 电子邮件服务器应监控收发电子邮件中是否含有病毒，并自动采取相应处理措施；

b） 应建立有效的机制防范垃圾邮件，例如垃圾邮件投诉处理机制等，确保正常用户邮件业务的使用；

c） 应对用户收发邮件等操作进行日志记录，以便需要时能够查询相关信息，应避免相关数据和信息被篡改和破坏。

8.2.1.5.3 FTP 安全要求

a） FTP服务器应监控用户上传文件中是否含有病毒，并自动采取相应的处理措施；

b） 应防止用户对FTP服务器进行非法读写，应拒绝由未被允许的IP地址、用户名、子网域发来的FTP操作请求，应能够限制单个IP地址、IP地址段、用户名、子网域的连接数量和连接频率；

c） 应对用户上传下载文件等操作进行日志记录，以便需要时能够查询相关信息，应避免相关数据和信息被篡改和破坏。

8.2.1.5.4 公众信息发布安全要求

公众信息发布是指用户通过互联网实现的个人或公共信息发布，如博客、播客、电子公告、威克、维克等，发布的信息包括文本、图片、音频、视频文件等等。公众信息发布安全要求包括：

a） 对公众提供信息发布服务的平台应实时监控用户发布和评论的文字、图片、音频、视频文件中是否含有病毒，并自动采取相应的处理措施。

b） 对公众提供信息发布服务的平台应对向公众发布的各种文本信息内容进行实时的过滤，以阻止有害信息的传播；应采用技术或人工手段有效防止其他类型（图像、音频、视频等）有害信息通过业务网络向公众传播。

c） 应建立有害信息检查机制和投诉处理制度。

d） 应记录向公众发布的信息内容及其发布时间、互联网地址或者域名等，并保存60日（业务日志的内容和保留期限参照《互联网信息服务管理办法》，如果该法规修订，则本标准应作相应改动），以便需要时能够查询相关信息，应避免相关数据和信息被篡改和破坏。

e） 应对用户发布信息、浏览信息、评论、下载等操作进行日志记录，以便需要时能够查询相关信息，应避免相关数据和信息被篡改和破坏。

8.2.1.6 在线数据处理与交易处理安全要求

参见YDN 126-2005《增值电信业务网络信息安全保障基本要求》附录D。

8.2.1.7 移动互联网信息服务安全要求

应根据服务类型，满足8.2.1.5节互联网信息服务的安全要求。

8.2.2 互联网设备安全要求

宽带网络接入服务器的具体设备安全要求参见YD/T 1658-2007，网络接入服务器的具体设备安全要求参见YD/T 1045-2000的安全要求，电子邮件服务器的具体设备安全要求参见YD/T 1311-2004，用户端网络设备的具体安全要求参见YD/T 1746-2008《IP承载网安全防护要求》8.3节。

8.2.3 互联网物理环境安全要求

应满足YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》第2级要求。

8.2.4 互联网管理安全要求

应满足YD/T 1756-2008《电信网和互联网管理安全等级保护要求》第2级要求。

8.3 第3.1级要求

8.3.1 互联网业务及应用安全要求

8.3.1.1 通用安全要求

除满足8.2.1.1节的要求之外，还应满足：

a） DNS服务器、Web服务器、电子邮件服务器、FTP服务器、公众信息发布服务器、在线数据处理与交易处理服务器、数据库服务器等互联网业务及应用系统的相关服务器应具有高可靠性、高稳定性、高维护性和一定冗余性；

b） 应配备多台相关服务器，应有相应的数据备份机制，保证在个别服务器发生故障或升级系统时不会引起互联网业务/应用的中断或系统瘫痪；

c） 在向用户提供业务/应用之前，应使用加密技术进行用户认证；

d） 互联网业务及应用系统的用户端网络安全具体要求参见YD/T 1746-2008《IP承载网安全防护要求》第3.1级要求。

8.3.1.2 互联网域名服务安全要求

除应满足8.2.1.2节的要求之外，还应满足：

a） 所提供域名解析服务应具有一定的可恢复性，在服务中断后，应在保证8.2.1.2节 c）的要求范围内尽快恢复域名解析服务；

b） 应有重要数据例如域名信息的备份机制，以便相关数据被破坏后，能够及时恢复服务；

c） 应能根据日志信息进行入侵检测和入侵企图分析，当检测到入侵行为时，应记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

8.3.1.3 互联网数据中心安全要求

除应满足8.2.1.3节的要求之外，还应满足：

a） 互联网数据中心某个客户的服务异常不应导致为其他客户提供服务的异常；

b） 如果按照客户要求记录了相关服务器的操作访问日志，应能根据日志信息进行入侵检测和入侵企图分析，当检测到入侵行为时，应记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

8.3.1.4 互联网接入服务安全要求

除应满足8.2.1.4节的要求之外，还应满足：

a） 宽带网络接入服务器或网络接入服务器应通过用户名等方式识别并确认用户的身份，应可选择不同的认证协议对用户进行身份验证，应设置不同的访问控制策略来控制用户的接入，应能够控制用户对资源的访问，不允许用户过量占用资源；

b） 宽带网络接入服务器应支持VPN功能。

8.3.1.5 互联网信息服务安全要求

8.3.1.5.1 Web 浏览安全要求

除应满足8.2.1.5.1节的要求之外，还应满足：

a） 应拒绝由未被允许的IP地址、子网域发来的浏览请求，应拒绝访问Web服务器上不公开的内容，应对各种形式执行程序的访问进行控制；

b） 应能根据日志记录进行入侵检测和入侵企图分析，当检测到入侵行为时，应记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

8.3.1.5.2 电子邮件安全要求

除应满足8.2.1.5.2节的要求之外，还应满足：

a） 应支持强制SMTP认证，应支持关闭自动转发电子邮件的功能；

b） 应拒绝由未被允许的IP地址、用户名、子网域发来的电子邮件服务连接请求，应支持黑名单和白名单功能，应拒绝电子邮件转发次数超过预定上限的电子邮件的继续转发操作，应拒绝收信人数量超过预定上限的电子邮件的发送操作，应拒绝附件数量超过预定上限的电子邮件的发送操作，应拒绝邮件大小超过预定上限的电子邮件的发送操作，应限制单个IP地址或用户名的连接数量和连接频率；

c） 应对进入电子邮件服务器的电子邮件地址、标题等关键信息进行扫描、检测、过滤、拦截，并向用户通知相关处理结果；

d） 应能根据日志记录进行入侵检测和入侵企图分析，当检测到入侵行为时，应记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

8.3.1.5.3 FTP 安全要求

除应满足8.2.1.5.3节的要求之外，还应满足：

a） 应能够对一个访问账户或一个请求进程占用的资源进行限制；

b） 应能根据日志记录进行入侵检测和入侵企图分析，当发现入侵行为时，应记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

8.3.1.5.4 公众信息发布安全要求

除应满足8.2.1.5.4节的要求之外，还应满足：

a） 应拒绝由未被允许的IP地址、用户名、子网域名发来的发布信息请求、浏览信息请求、评论请求和下载请求等；

b） 应能根据用户操作日志记录进行入侵检测和入侵企图分析，当发现入侵行为时，应记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

8.3.1.6 在线数据处理与交易处理安全要求

应满足8.2.1.6节的要求。

8.3.1.7 移动互联网信息服务安全要求

应根据服务类型，满足8.3.1.5节互联网信息服务的安全要求。

8.3.2 互联网设备安全要求

应满足8.2.2节的要求。

8.3.3 互联网物理环境安全要求

参见YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》中第3.1级的安全要求。

8.3.4 互联网管理安全要求

参见电信网和互联网管理安全等级保护要求中第3.1级的安全要求。

8.4 第 3.2 级要求

同第3.1级的要求。

8.5 第 4 级要求

同第3.2级要求。

8.6 第 5 级要求

待补充。

9 互联网灾难备份及恢复要求

9.1 互联网灾难备份及恢复等级

根据YD/T 1731-2008《电信网和互联网灾难备份及恢复实施指南》5.1节，灾难备份及恢复定级应与安全等级保护确定的安全等级一致。

9.2 第1级要求

不作要求。

9.3 第2级要求

9.3.1 互联网冗余系统、冗余设备及冗余链路要求

互联网业务及应用系统的灾难恢复时间应满足行业管理、网络和业务运营商应急预案相关要求。

9.3.2 互联网备份数据要求

a） 互联网业务及应用系统的关键数据（如业务数据、计费数据、系统配置数据、管理员操作维护记录、用户信息等）应有容灾数据备份；

b） 互联网业务及应用系统的数据备份范围和时间间隔、数据恢复能力应满足行业管理、网络和业务运营商应急预案相关要求。

9.3.3 互联网人员和技术支持能力要求

应有负责灾难备份及恢复的机房运行管理人员。

9.3.4 互联网运行维护管理能力要求

a） 应有针对灾难备份及恢复的机房运行管理制度；

b） 应有互联网业务及应用系统的介质存取、验证和转储的管理制度，确保相关服务器、用户端网络备份数据的授权访问。

9.3.5 互联网灾难恢复预案要求

互联网业务及应用系统应有完整的灾难恢复预案。

9.4 第3.1级要求

9.4.1 互联网冗余系统、冗余设备及冗余链路要求

除满足9.2.1节的要求之外，还应满足：

互联网业务及应用系统应具备一定的灾难恢复能力，应配备多台备份DNS服务器、备份域名注册/交易服务器、备份宽带网络接入服务器、备份网络接入服务器、备份Web服务器、备份电子邮件服务器、备份FTP服务器、备份公众信息发布服务器、备份在线数据处理与交易处理服务器、备份数据库服务器等，应有备份用户端网络设备和链路；在发生灾难时可采用冗余系统、冗余设备及冗余链路支持互联网业务及应用的提供。

9.4.2 互联网备份数据要求

应满足9.2.2节的要求。

9.4.3 互联网人员和技术支持能力要求

除满足9.2.3节的要求之外，还应满足：

互联网业务及应用系统应有负责灾难备份及恢复的技术人员。

9.4.4 互联网运行维护管理能力要求

除满足9.2.4节的要求之外，还应满足：

a） 互联网业务及应用系统应按介质特性对相关服务器、用户端网络备份数据进行定期的有效性验证；

b） 互联网业务及应用系统应有相关服务器、用户端网络的数据容灾备份管理制度。

9.4.5 互联网灾难恢复预案要求

除满足9.2.5节的要求之外，还应满足：

a） 互联网业务及应用系统应有灾难恢复预案的教育和培训；

b） 互联网业务及应用系统应有灾难恢复预案的演练。

9.5 第3.2级要求

与第3.2级的要求相同。

9.6 第4级要求

同第3.2级要求。

9.7 第5级要求

待补充。

参 考 文 献

YD/T 1728-2008	电信网和互联网安全防护管理指南
YD/T 1729-2008	电信网和互联网安全等级保护实施指南
YD/T 1731-2008	电信网和互联网灾难备份及恢复实施指南
YD/T 1742-2008	接入网安全防护要求
YD/T 1744-2008	传送网安全防护要求
YD/T 1746-2008	IP 承载网安全防护要求
YD/T 1754-2008	电信网和互联网物理环境安全等级保护要求
YD/T 1756-2008	电信网和互联网管理安全等级保护要求
YD/T 1658-2007	宽带网络接入服务器安全技术要求
YD/T 1045-2000	网络接入服务器技术规范
YD/T 1311-2004	防范互联网垃圾电子邮件技术要求
YD/T 126-2005	增值电信业务网络信息安全保障基本要求
国家标准	信息安全 信息系统安全等级保护基本要求（报批稿）
中华人民共和国信息产业部令（第 30 号）	中国互联网络域名管理办法
中华人民共和国国务院令（第 292 号）	互联网信息服务管理办法