ICS 35.110
M 11

YD

中华人民共和国通信行业标准

YD/T 2584-2013

互联网数据中心安全防护要求

Security protection requirements for internet data center

2013-07-22 发布　　2013-10-01 实施

中华人民共和国工业和信息化部　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。该系列标准预计结构及名称如下：

1. 《电信网和互联网安全防护管理指南》
2. 《电信网和互联网安全等级保护实施指南》
3. 《电信网和互联网安全风险评估实施指南》
4. 《电信网和互联网灾难备份及恢复实施指南》
5. 《固定通信网安全防护要求》
6. 《移动通信网安全防护要求》
7. 《互联网安全防护要求》
8. 《增值业务网—消息网安全防护要求》
9. 《增值业务网—智能网安全防护要求》
10. 《接入网安全防护要求》
11. 《传送网安全防护要求》
12. 《IP承载网安全防护要求》
13. 《信令网安全防护要求》
14. 《同步网安全防护要求》
15. 《支撑网安全防护要求》
16. 《非核心生产单元安全防护要求》
17. 《电信网和互联网物理环境安全等级保护要求》
18. 《电信网和互联网管理安全等级保护要求》
19. 《固定通信网安全防护检测要求》
20. 《移动通信网安全防护检测要求》
21. 《互联网安全防护检测要求》
22. 《增值业务网—消息网安全防护检测要求》
23. 《增值业务网—智能网安全防护检测要求》
24. 《接入网安全防护检测要求》
25. 《传送网安全防护检测要求》
26. 《IP承载网安全防护检测要求》
27. 《信令网安全防护检测要求》
28. 《同步网安全防护检测要求》
29. 《支撑网安全防护检测要求》
30. 《非核心生产单元安全防护检测要求》
31. 《电信网和互联网物理环境安全等级保护检测要求》
32. 《电信网和互联网管理安全等级保护检测要求》

33.《域名系统安全防护要求》
34.《域名系统安全防护检测要求》
35.《网上营业厅安全防护要求》
36.《网上营业厅安全防护检测要求》
37.《WAP网关系统安全防护要求》
38.《WAP网关系统安全防护检测要求》
39.《电信网和互联网信息服务业务系统安全防护要求》
40.《电信网和互联网信息服务业务系统安全防护检测要求》
41.《增值业务网 即时消息业务系统安全防护要求》
42.《增值业务网 即时消息业务系统安全防护检测要求》
43.《域名注册系统安全防护要求》
44.《域名注册系统安全防护检测要求》
45.《应用商城安全防护要求》
46.《应用商城安全防护检测要求》
47.《互联网内容分发网络安全防护要求》（本标准）
48.《互联网内容分发网络安全防护检测要求》
49.《互联网数据中心安全防护要求》
50.《互联网数据中心安全防护检测要求》

本标准与YD/T 2585-2013《互联网数据中心安全防护检测要求》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：工业和信息化部电信研究院、中国移动通信集团公司。

本标准主要起草人：魏　亮、周　智、卜　哲、曹一生。

互联网数据中心安全防护要求

1 范围

本标准规定了互联网数据中心在安全等级保护、安全风险评估、灾难备份及恢复等方面的安全防护要求。

本标准适用于公众电信网和互联网中的互联网数据中心。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 1478 电信管理网安全技术要求

YD/T 1729 电信网和互联网安全等级保护实施指南

YD/T 1754 电信网和互联网物理环境安全等级保护要求

YD/T 1756 电信网和互联网管理安全等级保护要求

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

互联网数据中心 Internet Data Center

互联网数据中心是基于Internet网络，为集中式收集、存储、处理和发送数据的设备提供运行维护的设施以及相关的服务体系。IDC提供的主要业务包括主机托管（机位、机架、VIP机房出租）、资源出租（如虚拟主机业务、数据存储服务）、系统维护（系统配置、数据备份、故障排除服务）、管理服务（如带宽管理、流量分析、负载均衡、入侵检测、系统漏洞诊断），以及其他支撑、运行服务等。

3.1.2

互联网数据中心安全等级 Security Classification of IDC

互联网数据中心安全重要程度的表征。重要程度可从互联网数据中心受到破坏后，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。

3.1.3

互联网数据中心安全等级保护 Classified Security Protection of IDC

对互联网数据中心分等级实施安全保护。

3.1.4

组织 Organization

由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。

3.1.5

互联网数据中心安全风险　Security Risk of IDC

人为或自然的威胁可能利用互联网数据中心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。

3.1.6

互联网数据中心安全风险评估　Security Risk Assessment of IDC

指运用科学的方法和手段，系统地分析互联网数据中心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。防范和化解互联网数据中心安全风险，或者将风险控制在可接受的水平，为最大限度地保障互联网数据中心的安全提供科学依据。

3.1.7

互联网数据中心资产　Asset of IDC

互联网数据中心中具有价值的资源，是安全防护保护的对象。互联网数据中心中的资产可能是以多种形式存在，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，如互联网数据中心Web服务器等。

3.1.8

互联网数据中心资产价值　Asset Value of IDC

互联网数据中心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。

3.1.9

互联网数据中心威胁　Threat of IDC

可能导致对互联网数据中心产生危害的不希望事故件在起因，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。常见的互联网数据中心威胁有黑客入侵、硬件故障、人为操作失误、火灾、水灾等。

3.1.10

互联网数据中心脆弱性　Vulnerability of IDC

互联网数据中心中存在的弱点、缺陷与不足，不直接对资产造成危害，但可能被威胁所利用从而危害资产的安全。

3.1.11

互联网数据中心灾难　Disaster of IDC

由于各种原因，造成互联网数据中心故障或瘫痪，使互联网数据中心的功能停顿或服务水平不可接受的突发性事件。

3.1.12

互联网数据中心灾难备份　backup for disaster recovery of IDC

为了互联网数据中心灾难恢复而对相关网络要素进行备份的过程。

3.1.13

互联网数据中心灾难恢复　Disaster Recovery of IDC

为了将互联网数据中心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。

3.1.14

中间件 Middle Ware

一种独立的系统软件或服务程序，中间件位于客户机/ 服务器的操作系统之上，管理计算机资源和网络通信，是连接两个独立应用程序或独立系统的软件，针对不同的操作系统和硬件平台，中间件可以有符合接口和协议规范的多种实现。实现互联网数据中心功能的应用程序运行在中间件之上，此时中间件包括Web服务器和应用服务器功能模块。

3.1.15

跨站脚本攻击 Cross-Site Scripting

入侵者在远程Web页面的HTML代码中插入具有恶意目的的数据，用户认为该页面是可信赖的，但是当浏览器下载该页面，嵌入其中的脚本将被解释执行，从而威胁用户浏览过程的安全。

3.1.16

SQL注入攻击 SQL Injection Attack

攻击者构造恶意的字符串，欺骗应用系统用于构造数据库查询语句并执行，从而达到盗取或修改数据库中存储的数据的目的。

3.1.17

路径遍历攻击 Path Traversal Attack

攻击者操纵输入参数使应用系统执行或透露任意文件内容，或对服务器任意文件目录进行读、写、删除等操作。

3.1.18

命令注入攻击 Command Injection Attack

命令注入攻击是指攻击者操纵输入参数使应用系统执行额外的指令，例如操作系统命令等。

3.2 缩略语

下列缩略语适用于本文件。

ACL	Access Control List	访问控制列表
CC	Challenge Collapsar	挑战黑洞
CPU	Central Processing Unit	中央处理器
DDOS	Distributed Denial of Service	分布式拒绝服务
FTP	File Transfer Protocol	文件传输协议
ICMP	Internet Control Message Protocol	Internet 控制报文协议
IDC	Internet Data Center	互联网数据中心
IP	Internet Protocol	网络之间互连的协议
MAC	Medium Access Control	媒体介入控制层
SQL	Structured Query Language	结构化查询语言
SSH	Secure Shell	安全协议外壳
SSL	Secure Sockets Layer	安全套接层

UDP Flood	User Datagram Protocol Flood	UDP 洪水攻击
URL	Uniform Resource Locator	统一资源定位符
uRPF	Unicast Reverse Path Forwarding	单播逆向路径转发
VLAN	Virtual Local Area Network	虚拟局域网

4 互联网数据中心安全防护概述

4.1 互联网数据中心安全防护范围

为用户提供各种IDC服务包括IP网络、主机、服务器、安全设备等在内的IDC基础设施，和为了保证IDC正常运行所构建的包括集中配置、集中监控、计费、灾备等在内的IDC支撑系统，以及为了保证IDC网络安全所构建的IDC网络安全防护系统。

4.2 互联网数据中心安全风险分析

4.2.1 资产分析

互联网数据中心的资产可分为设备硬件、软件、数据、网络、服务、文档和人员等，详见附录A对资产的分类及举例，其中重点资产如下：

1）互联网数据中心中的各种软硬件设备，如主机设备，网络设备、操作系统、数据库、中间件、应用程序、支撑系统等；

2）互联网数据中心中的重要数据，保存在互联网数据中心的各种重要信息数据，用户信息（用户登录ID、用户在互联网数据中心上的操作记录等）、设备配置数据、管理员操作维护记录等；

3）互联网数据中心中的重要服务，这些服务至少包括主机托管（机位、机架、VIP机房出租）、资源出租（如虚拟主机业务、数据存储服务）、系统维护（系统配置、数据备份、故障排除服务）、管理服务（如带宽管理、流量分析、负载均衡、入侵检测、系统漏洞诊断）。

4.2.2 资产脆弱性分析

互联网数据中心的脆弱性可分为技术脆弱性和管理脆弱性两方面，见附录 A 中的互联网数据中心的脆弱性列表。

4.2.3 安全威胁分析

互联网数据中心的威胁可分为业务威胁、设备威胁、环境威胁和人为威胁，其中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，详见附录A中的互联网数据中心的威胁列表。

4.2.4 安全风险分析

互联网数据中心面临来自公众互联网上及内部的各种安全威胁，自身脆弱性一旦被利用后将产生很大的安全风险。

4.2.4.1 设备安全风险

互联网数据中心中网络设备的安全风险主要来自两个方面，一个是设备自身的安全风险，另外一个是外界环境的安全风险。具体的设备安全风险如下：

a）设备自身的安全缺陷或未能够及时修复的安全缺陷，导致针对该设备的缺陷利用，影响 IDC 业务的连续性、可靠性和完整性；

b）承载业务系统硬件、网络环境等方面的风险；

c）业务系统自身安全风险。

4.2.4.2 网络安全风险

互联网数据中心网络的安全风险主要如下：

a）来自内部和外部可能的网络攻击，如 DDoS 攻击、利用系统漏洞进行的各类攻击等；

b）蠕虫病毒入侵，局域网内部病毒等恶意软件的传播，尤其是维护终端、磁盘介质使用等导致的病毒扩散；

c）利用管理和技术漏洞，或者内部资源成为僵尸网络、木马的被控资源，IDC 资源被用作攻击外部网络的工具；

d）Web 类应用被挂马，成为木马大范围传播的主要途径；

e）由于对 IDC 网络进行维护不恰当，而导致的安全风险。

4.2.4.3 应用层安全风险

互联网数据中心涉及应用层的安全风险主要来自以下两个方面：

a）来自原互联网、内部恶意用户的安全风险；

b）IDC 客户或者 Web 用户发布反动、色情、违反版权要求、进行人身攻击的文字、视频、图片、音频、游戏等。

4.2.4.4 数据安全风险

4.2.4.4.1 网管数据

互联网数据中心网管数据，主要指互联网数据中心管理层面的数据，其安全风险主要如下：

a）数据传输过程中被窃取，篡改、破坏；

b）越权访问；

c）病毒入侵导致丢失；

d）其他误操作、系统故障、介质问题等原因导致的数据丢失、泄漏。

4.2.4.4.2 内部业务数据

互联网数据中心内部业务数据，主要指互联网数据中心各个业务区域数据，其安全风险一方面来自于各个业务的不同要求，另外更主要的一方面是这些业务数据的存放，具体如下：

a）病毒、木马、间谍软件的入侵；

b）针对敏感数据的非法篡改、获取；

c）数据的存储安全风险，包括数据存储磁盘管理不善，数据访问管理不善带来的风险等。

4.2.4.4.3 帐号口令

a）口令密码明文保存导致失窃；

b）弱口令导致的暴力破解；

c）网络监听明文传输的账号口令。

4.3 互联网数据中心安全防护内容

互联网数据中心已成为互联网时代重要不可缺少的重要基础性设施。互联网数据中心自身安全性、对其所提供各类服务的安全管控、支撑系统的安全防护是互联网数据中心安全防护的重要内容，具体包括：业务安全、网络安全、主机安全、中间件安全、安全域边界安全、集中运维安全管控系统安全、物理环境安全、管理安全。

5 互联网数据中心定级对象和安全等级确定

网络和业务运营商应根据YD/T 1729中确定安全等级的方法对互联网数据中心进行定级，即根据社会影响力、所提供服务的重要性、规模和服务范围的大小对互联网数据中心分别定级，定级方法中的权重α、β、γ可根据具体网络情况进行调节。建议权重值α、β、γ分别为：0.4、0.4、0.2，或者1/3、1/3、1/3，各IDC运营企业也可根据本企业实际情况调节α、β、γ3个权重值。

（1） 社会影响力 I

根据 YD/T 1729，社会影响力表示定级对象受到破坏后对国家安全、社会秩序、经济运行、公共利益的损害程度。IDC 服务对象可能是国家机关部委、企事业单位、企业网站等。建议服务于国家重要部委、重要金融机构、国家级网络媒体、大型互联网域名服务商等的 IDC 社会影响力赋值为 4，服务于省级政府、一般金融机构、大型网站（如 Alexa 排名前 50）等的 IDC 社会影响力赋值为 3，服务于其他政府、企事业单位或一般网站等的 IDC 社会影响力赋值为 2。

（2） 规模和服务范围 R

根据 YD/T 1729，规模表示定级对象服务的用户数多少，服务范围表示定级对象服务的地区范围大小。建议从 IDC 服务对象指标衡量 IDC 规模和服务范围，IDC 服务对象是国家机关部委、企事业单位、企业网站等。建议服务于国家重要部委、重要金融机构、国家级网络媒体、大型互联网域名服务商等的 IDC 社会影响力赋值为 4，服务于省级政府、一般金融机构、大型网站（如 Alexa 排名前 50）等的 IDC 社会影响力赋值为 3，服务于其他政府、企事业单位或一般网站等的 IDC 社会影响力赋值为 2。

（3） 所提供服务的重要性 V

根据 YD/T 1729，所提供服务的重要性表示定级对象提供的服务被破坏后对网络和业务运营商的合法权益的影响程度。建议从 IDC 服务对象指标衡量 IDC 提供服务的重要性，IDC 服务对象是国家机关部委、企事业单位、企业网站等。建议服务于国家重要部委、重要金融机构、国家级网络媒体、大型互联网域名服务商等的 IDC 社会影响力赋值为 4，服务于省级政府、一般金融机构、大型网站（如 Alexa 排名前 50）等的 IDC 社会影响力赋值为 3，服务于其他政府、企事业单位或一般网站等的 IDC 社会影响力赋值为 2。

6 互联网数据中心安全防护保护要求

6.1 第 1 级要求

6.1.1 业务安全

不作要求。

6.1.2 网络安全

6.1.2.1 结构安全

不作要求。

6.1.2.2 访问控制

不作要求。

6.1.2.3 安全审计

不作要求。

6.1.2.4 入侵防范

a）应面向互联网部署防火墙等安全防护设备，及时发现安全事件；

b）应在互联网数据中心与互联网接口处具备流量监控分析能力，以及时发现导致流量异常的安全事件；

c）应在IDC实施虚假源地址流量控制策略，包括但不限于：在IDC出口设备上开启uRPF（单播逆向路径转发）功能，对于不具备开启条件的设备，启用ACL（访问控制列表）功能过滤虚假源地址。

d）应在完成对IDC业务及客户源地址的备案和梳理。

6.1.2.5 网络设备防护

不作要求。

6.1.3 主机安全

不作要求。

6.1.4 中间件安全

不作要求。

6.1.5 安全域边界安全

应根据互联网数据中心的生产运行、操作维护、系统管理等功能，采用交换机、路由器、防火墙等设备，利用VLAN划分、IP网段划分、可信任域等划分等方式对互联网数据中心内部网络划分安全域，并对跨域的访问实施针对访问源MAC地址、源IP地址、端口号等信息的控制策略。

6.1.6 集中运维安全管控系统安全

a）互联网数据中心集中运维安全管控系统应与提供互联网数据中心各种服务的互联网数据中心基础设施隔离，应部署在不同网络区域，网络边界处设备应按不同互联网数据中心业务需求实施访问控制策略，应只开放管理所必须的服务及端口，避免开放较大的IP地址段及服务；

b）互联网数据中心集中运维安全管控系统应采用安全的管理和控制信息的分发、过滤机制；网络管理信息应通过加密传送；对于专用管理接口，应对目的地址为设备本身的非管理报文和到数据业务接口的报文进行控制；

6.1.7 物理环境安全

应满足YDT 1754-2008中的第1级要求。

6.1.8 管理安全

应满足YDT 1756-2008中的第1级要求。

6.2 第2级要求

6.2.1 业务安全

除满足6.1.1的要求以外，还应满足：

a）按照合同保证互联网数据中心用户业务的安全；

b）具有对网络安全漏洞攻击监控能力，包括但不限于以下能力：

- 支持对已知安全漏洞攻击流量和攻击报文的检测；
- 支持对组合型攻击流量和攻击报文的检测和告警；
- 支持对攻击源的溯源和操作行为记录；
- 支持通过IP 5元组、攻击数据包类型、攻击报文关键字、攻击流量等对已知安全漏洞攻击的阻断；
- 支持对疑似安全漏洞攻击行为的研判和预警；

■ 支持对互联网数据中心机房服务器的 Web 网站挂马扫描；

c）应具备对 DDoS 攻击的监控能力，包括但不局限于以下能力：

■ 支持对常见 DDoS 攻击（如 SYN Flood、UDP Flood、ICMP Flood 等）的检测和告警；

■ 支持对 Web 应用层 DDoS 攻击（如 CC 攻击）的检测和告警；

■ 支持对 DDoS 攻击源或僵尸机的溯源和攻击行为记录；

■ 支持通过 IP 5 元组、包过滤、阈值限制、重定向等手段清洗 DDoS 攻击流量。

6.2.2 网络安全

6.2.2.1 结构安全

a）应绘制与当前运行情况相符的网络拓扑结构图（反映互联网接口、内部网络划分等）；

b）应保证网络单元关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要。

6.2.2.2 访问控制

满足 7.1.2.2 的要求以外，还应满足：

a）应对互联网与网络单元接口的流量进行监控统计；

b）互联网数据中心与互联网接口处的流量带宽应具备冗余空间，满足业务高峰期需要。

6.2.2.3 安全审计

a）应对网络系统中的关键网络设备运行状况、网络流量、用户行为等进行日志记录；

b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

6.2.2.4 入侵防范

a）应在互联网数据中心与互联网的网络边界处检测、防御以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；

b）实现安全划分的网络边界设备、主机的安全日志应在本地或外部设备上进行记录、输出、存储，并及时、定期审计安全域边界安全防护设备的日志，日志审计范围应该覆盖设备自身操作维护记录，以及设备对外部发起行为的记录，应形成、储存相关的审计文档。

6.2.2.5 网络设备防护

a）应对登录网络设备的用户进行身份鉴别；

b）应对网络设备的管理员登录地址进行限制；

c）网络设备用户的标识应唯一；

d）身份鉴别信息应具有不易被冒用的特点，口令应有一定复杂度（长度至少8位，是数字、大写字母、小写字母的组合），并定期（更换周期小于90天）更换；

e）应具有登录失败处理功能，可采取结束会话、限制登录失败次数和当网络登录连接超时自动退出等措施；

f）当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

6.2.3 主机安全

6.2.3.1 身份鉴别

a）应对登录操作系统和数据库系统的用户进行身份标识和鉴别；

b）操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有一定复杂度（长度至少8位，是数字及字母的组合，并对字母大小写敏感），并定期（更换周期小于90天）更换；

c）应启用登录失败处理功能，可采取结束会话、限制登录失败次数和自动退出等措施；

d）当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；

e）应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。

6.2.3.2 访问控制

a）应实现操作系统和数据库系统特权用户的权限分离；

b）应限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令；

c）应及时删除多余的、过期的账户，避免共享账户的存在。

6.2.3.3 安全审计

a）审计范围应覆盖到主机上的每个操作系统用户和数据库用户；

b）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；

c）审计记录应包括事件的日期、时间、类型和结果等；

d）应保护审计记录，避免受到未预期的删除、修改或覆盖等。

6.2.3.4 入侵防范

操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，保持系统补丁及时得到更新。

6.2.3.5 恶意代码防范

应尽量安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。

6.2.3.6 资源控制

a）应通过设定终端接入方式、网络地址范围等条件限制操作维护终端远程登录；

b）应根据安全策略设置登录终端的操作超时锁定。

6.2.4 中间件安全

6.2.4.1 身份鉴别

应实现操作系统和中间件用户的权限分离，中间件应使用独立用户。

6.2.4.2 访问控制

中间件使用的操作系统级别的服务用户的权限应遵循最小权限原则。

6.2.4.3 安全审计

a）应采用技术手段如定期运行文件完整性监控软件，及时发现中间件关键系统数据或文件被非授权更改并通知相关人员；应至少每周对关键文件进行比对；

b）审计中间件安全日志。

6.2.4.4 入侵防范

a）中间件的安装应遵循最小安装的原则，应关闭或限制与系统正常运行无关，但可能造成安全隐患的默认扩展功能，例如示例程序、后台管理、不必要的存储过程等；

b）应禁用中间件的目录列出功能；

c）协议级的配置时应禁用中间件的不必要的HTTP方法，例如PUT，TRACE，DELETE等，若启用了HTTPS则应禁用HTTP；

d）应启用必要的语言安全设置，例如PHP语言设置，JAVA语言设置；

e）对安装时自动生成的帐号（如：演示账号）须做清理或者修改密码。

6.2.5 安全边界要求

除了满足 7.1.5 节的要求外，还应该加强边界安全隔离与防护，加强对边界设备的日志及审计的安全防护工作。安全边界包括互联网数据中心网络单元与外部网络之间的安全边界以及 IDC 网络单元内部不同安全等级安全域之间的边界。

6.2.5.1 边界安全隔离与防护

a）通过运营企业内部网络如DCN网络远程访问互联网数据中心中设备，应按业务需求在被访问的IP网网络边界设备上实施接入访问控制策略，应逐一对至少包括源IP地址、端口号在内的控制项进行限制，避免开放过长IP地址段；二层协议漏洞（划分、安全监控）；

b）通过公共互联网远程访问互联网数据中心中设备，必须使用安全的VPN方式，并按业务需求在被访问的IP网网络边界设备上实施接入访问控制策略，应逐一对至少包括源MAC地址、源IP地址、端口号在内的控制项进行限制，避免开放过长IP地址段及过多端口；

c）对于目的地址为IP网网络内IP地址的数据包，安全域边界应具有有效的攻击识别和防范能力，应能具有对于异常数据流量的识别和处理能力；

d）网络单元边界隔离设备如采用Web方式进行配置管理，应使用用户安全鉴别和认证措施。防止Web等安全漏洞，如SQL注入、跨站脚本攻击。应保证配置安全，采取隐蔽Web后台配置页面等措施，防止后台配置界面泄露、Web路径泄露等漏洞被非法利用进行对设备的攻击入侵；

e）启用其他设备（主机隔离等）进行安全边界划分、隔离的应尽量实现严格的访问控制策略。

6.2.6 集中运维安全管控系统安全

除满足6.1.6的要求以外，还应该满足：

a）互联网数据中心支撑系统及安全防护系统应使用用户安全鉴别和认证措施，应符合YD/T 1478中相关安全技术要求，使用的SNMP协议原则应支持SNMPv3并支持VACM和USM等安全机制，对于远程登录应支持SSH以及其他相关加密和认证算法，对于Web管理应支持SSL/TLS等安全协议；

b）互联网数据中心支撑系统及安全防护系统中的设备支持的SNMP、SSH等服务应在非必要情况下关闭和禁用，必须使用SNMP协议的相关设备应加强对SNMP write写操作的管理控制，可采用增加Community的复杂度或采用ACL控制等其他方式；

c）互联网数据中心支撑系统及安全防护系统应能对节点、链路和各类资源的预警、告警、故障进行及时有效的定位，各类相关的预警阈值设置合理；

d）互联网数据中心支撑系统及安全防护系统应具有启用功能完整的系统安全日志功能；

e）互联网数据中心支撑系统及安全防护系统如采用Web技术进行配置、管理，应使用用户安全鉴别和认证措施，应防止Web等安全漏洞，如SQL注入、跨站脚本攻击，应保证配置安全，采取隐蔽Web后台配置页面等措施，防止后台配置界面泄露、Web路径泄露等漏洞被非法利用进行对设备、系统的攻击入侵。

6.2.7 灾难备份以及恢复

6.2.7.1 冗余系统、冗余设备及冗余链路

a）互联网数据中心应具备一定的抗灾难以及灾难恢复能力，重要服务器、重要部件、重要数据库应当采用本地双机备份的方式进行容灾保护；

b）互联网数据中心网络灾难恢复时间应满足行业管理、网络和业务运营[illegible]急预案的相关要求。

6.2.7.2 数据备份

a）互联网数据中心重要信息数据应提供本地备份；

b）互联网数据中心的数据备份范围和时间间隔、数据恢复能力应符合网络和业务运营商应急预案的相关要求。

6.2.8 物理环境安全

应满足 YDT 1754-2008 中的第 2 级要求，在本标准与企业规范标准、企业具体操作维护规范等文档对相同内容有重复要求时，采取从严原则，应符合最严格的安全要求。

6.2.9 管理安全

除满足 YDT 1756-2008 中的第 2 级要求外，还应该满足以下要求。

6.2.9.1 安全管理要求

a）至少覆盖但不限于安全管理制度、安全管理机构、人员安全管理、安全建设管理、安全运维管理等管理方面；

b）在本标准与企业规范标准、企业具体操作维护规范等文档对相同内容有重复要求时，采取从严原则，应符合最严格的安全要求。

6.2.9.2 人员和技术支持能力

a）IDC 应有安全管理人员和各类技术人员；

b）相关技术人员定期进行灾难备份及恢复方面的技能培训。

6.2.9.3 运行维护管理能力

a）IDC 应有介质存取、验证和转储管理制度，确保备份数据授权访问；

b）IDC 应按介质特性对备份数据进行定期的有效性验证；

c）IDC 应有相关服务器设备的灾难备份及恢复的管理制度。

6.2.9.4 灾难恢复预案

a）IDC 应有完整的灾难恢复预案；

b）IDC 应有灾难恢复预案的教育和培训，相关人员应了解灾难恢复预案并具有对灾难恢复预案进行实际操作的能力；

c）IDC 应有灾难恢复预案的演练，并根据演练结果对灾难恢复预案进行修正。

6.3 第 3.1 级要求

6.3.1 业务安全

除满足6.2.1的要求外，还应满足：

应具有对僵尸网络、木马和蠕虫监控的监控能力，包括但不限于以下能力：

- 支持对已知僵尸网络、木马和蠕虫病毒的检测和告警；
- 支持对压缩流量和嵌入型僵尸网络和木马的检测和告警；
- 支持对僵尸网络和木马控制端的溯源和操作行为记录；
- 支持对疑似僵尸网络、木马和蠕虫病毒的研判和预警；
- 支持通过 IP 5 元组、协议、域名或 URL 对已知僵尸网络、木马和蠕虫病毒的阻断；
- 支持对 IDC 机房服务器的 Web 网站挂马扫描；
- 支持基于网络行为、样本特征和恶意 URL 的僵尸网络、木马和蠕虫病毒库。

6.3.2 网络安全

6.3.2.1 结构安全

除满足 6.2.2.1 的要求以外，还应满足：

互联网数据中心的 Web 服务器、后台数据库应分开部署在不同物理主机上。

6.3.2.2 访问控制

与6.3.2.2要求相同。

6.3.2.3 安全审计

除满足 6.2.2.3 的要求之外，还应满足：

a）能够根据记录数据进行分析，并生成审计报表；

b）对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

6.3.2.4 入侵防范

除满足 6.2.2.4 的要求之外，还应满足：

当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应能够实时报警。

6.3.2.5 网络设备防护

除满足6.2.2.6的要求之外，还应满足：

a）应实现设备特权用户的权限分离；

b）身份鉴别信息应具有不易被冒用的特点，口令应有一定复杂度（长度至少8位，是数字、大写字母、小写字母、特殊字符中任意3种的组合），并定期（更换周期小于60天）更换。

6.3.2.6 恶意代码防范

除满足 6.2.2.7 的要求之外，还应满足：

a）在网络边界处对恶意代码进行检测和清除；

b）维护恶意代码库的升级和检测系统的更新；

c）对主机防恶意代码软件及网络设备防恶意代码软件进行统一管理。

6.3.3 主机安全

6.3.3.1 身份鉴别

除满足 6.2.3.1 的要求之外，还应满足：

操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有一定复杂度（长度至少8位，是数字、大写字母、小写字母、特殊字符中任意3种的组合），并定期（更换周期小于60天）更换。

6.3.3.2 访问控制

除满足6.2.3.2的要求之外，还应满足：

a）根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；

b）依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

6.3.3.3 安全审计

除满足6.2.3.3的要求之外，还应满足：

a）能够根据记录数据进行分析，并生成审计报表；

b）保护审计进程，避免受到未预期的中断。

6.3.3.4 入侵防范

除满足6.2.3.4的要求之外，还应满足：

能够检测到对IDC内主机进行入侵的行为，能够记录入侵的源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。

6.3.3.5 恶意代码防范

与6.3.2.5的要求相同。

6.3.3.6 资源控制

除满足6.2.3.6的要求之外，还应满足：

应对IDC内重要主机进行监视，包括监视主机的CPU、硬盘、内存、网络等资源的使用情况。

6.3.4 中间件安全

与6.2.4的要求相同。

6.3.5 安全域边界要求

与6.2.5的要求相同。

6.3.6 集中运维安全管控系统安全

与6.2.6的要求相同。

6.3.7 灾难备份以及恢复

与6.2.7的要求相同。

6.3.8 物理环境安全

应满足YDT 1754-2008中的第3.1级要求及本标准6.2.8节要求。

6.3.9 管理安全

除满足6.2.9外，还应该满足以下要求。

6.3.9.1 安全建设管理

a）IDC业务实施时，客户应提交业务客户信息采集表，主要包含但不限于以下信息：系统数据分类与安全等级、系统对基础设施的依赖关系、系统要求配置的防火墙与路由器策略等；

b）安全运维管理；

c）应至少每6个月检查一次防火墙和路由器的规则设置；

d）应至少每3个月进行一次应用层弱点扫描，当基础设施或应用完成重大的升级或调整后，应执行应用层弱点扫描；

e）应至少每年进行一次应用层渗透测试，当基础设施或应用完成重大的升级或调整后，应执行应用层渗透测试。

6.4 第3.2级要求

6.4.1 业务安全

与6.3.1的要求相同。

6.4.2 网络安全

与6.3.2的要求相同。

6.4.3 主机安全

与6.3.3的要求相同。

6.4.4 中间件安全

与6.3.4的要求相同。

6.4.5 安全域边界要求

与6.3.5的要求相同。

6.4.6 集中运维安全管控系统安全

与6.3.6的要求相同。

6.4.7 灾难恢复以及备份

6.4.7.1 冗余系统、冗余设备及冗余链路

除满足6.3.7的要求相同外，还应满足：

a）互联网数据中心应具备一定的抗灾难以及灾难恢复能力，重要服务器、重要部件、重要数据库应当采用异址（同城不同地点的机房或异地）方式进行容灾保护；

b）互联网数据中心与互联网之间应具备冗余链路；

c）互联网数据中心网络中关键设备之间应当提供多条物理链路（如 Web 服务器设备与数据库服务器设备之间）。

6.4.7.2 数据备份

除满足6.3.7的要求之外，还应满足：

互联网数据中心重要信息数据应提供异址备份（同城不同地点的机房或异地）。

6.4.7.3 人员和技术支持能力

与6.3.7的要求相同。

6.4.7.4 运行维护管理能力

与6.3.7的要求相同。

6.4.7.5 灾难恢复预案

除满足6.3.7的要求之外，还应满足：

互联网数据中心应有完善的灾难恢复预案管理制度。

6.4.8 物理环境安全

应满足YDT 1754-2008中的第3.2级要求。

6.4.9 管理安全

应满足YDT 1756-2008中的第3.2级要求。

6.5 第 4 级要求

同第 3.1 级要求。

6.6 第 5 级要求

待补充。

附 录 A
（规范性附录）
互联网数据中心安全风险分析

本附录指导互联网数据中心安全风险分析过程中的资产、脆弱性、威胁分析。

表A.1 互联网数据中心资产列表

分 类	示 例
设备硬件	互联网数据中心中的各种主机设备，网络设备
设备软件	设备中的软件，包括：操作系统、数据库软件、中间件软件（Web服务器软件、应用层服务器软件）、互联网数据中心应用软件、互联网数据中心支撑系统软件及其他应用软件等
重要数据	保存在互联网数据中心的各种重要信息数据，用户信息（用户登录ID、用户在互联网数据中心上的操作记录等）、设备配置数据、管理员操作维护记录等
网络	互联网数据中心的内部网络
服务	主机托管（机位、机架、VIP机房出租）、资源出租（如虚拟主机业务、数据存储服务）、系统维护（系统配置、数据备份、故障排除服务）、管理服务（如带宽管理、流量分析、负载均衡、入侵检测、系统漏洞诊断），以及其他支撑、运行服务
文档	纸质以及保存在电脑中的各种文件，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	管理人员，掌握重要技术的人员，如网络维护人员、设备维护人员、研发人员等

表A.2 互联网数据中心脆弱性列表

类型	对象	存在的脆弱性
技术脆弱性	服务/应用	由于网络和设备的处理或备份能力不够而导致服务提供不连续
	网络	设备性能低、运行不稳定；口令不够复杂、合理或没有经常更新；设备自身存在安全缺陷；设备所使用的资源存在被威胁利用的风险
	设备（软件、硬件和数据）	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；相关服务器不能记录敏感操作，或者相关日志功能没有启用或不够详细；不能提供帐号权限管理功能，不能提供账号修改界面；不能支持密码复杂度检测，或者密码未采用散列函数保存，而采用明文保存；业务流程设计方面的漏洞导致业务信息泄露和被滥用等。 数据传输未加密，容易被窃取、篡改；数据明文保存或者访问控制不严，存储介质保护不力等
	物理环境	机房的门禁、监控设备不完善；机房的设备老化；机房人员进出管理不严格等
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、对于外部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等

表A.3 互联网数据中心威胁列表

来　源		威胁描述
业务威胁		各种软件代码实现相关功能过程中的缺陷，导致对业务的认证、实现等造成的危害
设备威胁		各类设备本身的软硬件故障，设备和介质老化造成的数据丢失，系统宕机
环境威胁	物理环境	断电、静电、灰尘、潮湿、温度、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； 采用自主或内外勾结的方式盗窃或篡改机密信息； 外部人员利用恶意代码和病毒对网络或系统进行攻击； 外部人员进行物理破坏、盗窃等
	非恶意人员	内部人员由于缺乏责任心或者无作为而没有执行应当执行的操作，或无意地执行了错误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

YD/T 2584—2013

中华人民共和国
通信行业标准
互联网数据中心安全防护要求
YD/T 2584—2013

*

人民邮电出版社出版发行
北京市丰台区成寿寺路11号邮电出版大厦
邮政编码：100064
宝隆元（北京）印刷技术有限公司印刷

*

开本：880×1230　1/16　　2014年2月第1版
印张：1.5　　2014年2月北京第1次印刷
字数：37千字

15115·325
定价：20元