

ICS 33.040

M 10

YD

中华人民共和国通信行业标准

YD/T 2243-2016

代替 YD/T 2243-2011

电信网和互联网信息服务业务系统 安全防护要求

Security protection requirements for information
service system of telecom network and internet

2016-07-11 发布

2016-10-01 实施

中华人民共和国工业和信息化部 发布

电话 : 82054513 <http://www.ptsn.net.cn>

目 次

前 言.....II

1 范围.....1

2 规范性引用文件.....1

3 术语、定义和缩略语.....1

 3.1 术语和定义.....1

 3.2 缩略语.....2

4 信息服务业务系统安全防护概述.....2

 4.1 信息服务业务系统安全防护范围.....2

 4.2 信息服务业务系统安全风险分析.....3

 4.3 信息服务业务系统安全防护内容.....3

5 信息服务业务系统安全防护要求.....4

 5.1 第1级要求.....4

 5.2 第2级要求.....4

 5.3 第3级要求.....9

 5.4 第4级要求.....11

 5.5 第5级要求.....11

附录 A（规范性附录） 信息服务业务系统风险分析.....12

附录 B（规范性附录） 门户综合网站业务系统特定安全防护要求.....14

附录 C（规范性附录） 即时通信业务系统特定安全防护要求.....15

附录 D（规范性附录） 搜索系统特定安全防护要求.....16

附录 E（规范性附录） 信息社区服务系统的特定安全防护要求.....17

参考文献.....18

电话：82054513 <http://www.ptsn.net.cn>

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预计如下：

1. YD/T 1728 《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 1734-2009 《移动通信网安全防护要求》
8. YD/T 1735-2009 《移动通信网安全防护检测要求》
9. YD/T 1736-2009 《互联网安全防护要求》
10. YD/T 1737-2009 《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 1744-2009 《传送网安全防护要求》
18. YD/T 1745-2009 《传送网安全防护检测要求》
19. YD/T 1746-2014 《IP承载网安全防护要求》
20. YD/T 1747-2014 《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 1758-2008 《非核心生产单元安全防护要求》
28. YD/T 1759-2008 《非核心生产单元安全防护检测要求》
29. YD/T 1754-2008 《电信网和互联网物理环境安全等级保护要求》
30. 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》
31. YD/T 1756-2008 《电信网和互联网管理安全等级保护要求》
32. YD/T 1757-2008 《电信网和互联网管理安全等级保护检测要求》

33. YD/T 2052-2015 《域名系统安全防护要求》
34. YD/T 2053-2009 《域名系统安全防护检测要求》
35. YD/T 2092-2015 《网上营业厅安全防护要求》
36. YD/T 2093-2010 《网上营业厅安全防护检测要求》
37. YD/T 2241-2011 《WAP网关系统安全防护要求》
38. YD/T 2242-2011 《WAP网关系统安全防护检测要求》
39. YD/T 2243-2011 《电信网和互联网信息服务业务系统安全防护要求》（本标准）
40. YD/T 2244-2011 《电信网和互联网信息服务业务系统安全防护检测要求》
41. YD/T 2239-2011 《增值业务网一即时消息业务系统安全防护要求》
42. YD/T 2240-2011 《增值业务网一即时消息业务系统安全防护检测要求》
43. YD/T 2245-2011 《域名注册系统安全防护要求》
44. YD/T 2246-2011 《域名注册系统安全防护检测要求》
45. YD/T 2587-2013 《移动互联网应用商店安全防护要求》
46. YD/T 2588-2013 《移动互联网应用商店安全防护检测要求》
47. YD/T 2589-2013 《互联网内容分发网络安全防护要求》
48. YDB 115-2012 《互联网内容分发网络安全防护检测要求》
49. YD/T 2584-2013 《互联网数据中心安全防护要求》
50. YD/T 2590-2013 《互联网数据中心安全防护检测要求》
51. YD/T 2694-2014 《移动互联网应用安全防护要求》
52. YD/T 2695-2014 《移动互联网应用安全防护检测要求》
53. YD/T 2696-2014 《公众无线局域网安全防护要求》
54. YD/T 2697-2014 《公众无线局域网安全防护检测要求》
55. YD/T 2698-2014 《电信网和互联网安全防护基线配置要求及检测要求 网络设备》
56. YD/T 2699-2014 《电信网和互联网安全防护基线配置要求及检测要求 安全设备》
57. YD/T 2701-2014 《电信网和互联网安全防护基线配置要求及检测要求 操作系统》
58. YD/T 2700-2014 《电信网和互联网安全防护基线配置要求及检测要求 数据库》
59. YD/T 2702-2014 《电信网和互联网安全防护基线配置要求及检测要求 中间件》
60. YD/T 2703-2014 《电信网和互联网安全防护基线配置要求及检测要求 WEB应用系统》
61. YD/T 2692-2014 《电信和互联网用户个人电子信息保护通用技术要求和保护要求》
62. YD/T 2693-2014 《电信和互联网用户个人电子信息保护检测要求》
63. 《互联网接入服务安全防护要求》
64. 《互联网接入服务安全防护检测要求》
65. 《网络交易安全防护要求》
66. 《网络交易安全防护检测要求》
67. 《邮件系统安全防护要求》
68. 《邮件系统安全防护检测要求》
69. 《公有云服务安全防护要求》

YD/T 2243-2016

70. 《公有云服务安全防护检测要求》

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。

本标准按照GB/T 1.1-2009给出的规则起草。

本标准代替YD/T 2243-2011《电信网和互联网信息服务业务系统安全防护要求》。本标准与YD/T 2243-2011相比，除编辑性修改外主要技术变化如下：

- a) 修改了标准涉及范围（见第1章，2011年版的第1章）；
- b) 更新了规范性引用文件（见第2章，2011年版的第2章）；
- c) 更新了术语、定义和缩略语（见第3章，2011年版的第3章）；
- d) 完善了信息服务业务系统安全防护范围、安全风险分析和安全防护内容（见第4章）；
- e) 删除了“信息服务业务系统定级对象和安全等级确定”（2011年版的第5章）；
- f) 原第6章相关内容转移至附录A；
- g) 原第7章、原第8章合并为第5章，并进行了修订完善；
- h) 新增了附录B、附录C、附录D、附录E。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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：中国信息通信研究院、国家计算机网络应急技术处理协调中心、北京搜狐互联网信息服务有限公司、北京新浪互联信息服务有限公司、百度在线网络技术（北京）有限公司。

本标准主要起草人：封 莎、王 昕、林星辰、吴 婧、许章毅、高 磊、刘 亮。

本标准于2011年5月首次发布，本次为第一次修订。

电信网和互联网信息服务业务系统安全防护要求

1 范围

本标准规定了电信网和互联网信息服务业务系统分安全保护等级的安全防护要求,涉及到业务及应用安全、网络安全、设备及软件系统安全、物理安全和管理安全。

本标准适用于电信网和互联网信息服务业务系统。

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 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 2052-2009 域名系统安全防护要求
- YD/T 2584-2013 互联网数据中心安全防护要求
- YD/T 2589-2013 内容分发网(CDN)安全防护要求
- YD/T 2698-2014 电信网和互联网安全防护基线配置要求及检测要求 网络设备
- YD/T 2699-2014 电信网和互联网安全防护基线配置要求及检测要求 安全设备
- YD/T 2700-2014 电信网和互联网安全防护基线配置要求及检测要求 数据库
- YD/T 2701-2014 电信网和互联网安全防护基线配置要求及检测要求 操作系统
- YD/T 2702-2014 电信网和互联网安全防护基线配置要求及检测要求 中间件

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

信息服务业务系统安全风险 Security Risk of Information Service System

人为或自然的威胁可能利用信息服务业务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。

3.1.2

信息服务业务系统安全风险评估 Security Risk Assessment of Information Service System

运用科学的方法和手段,系统地分析信息服务业务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,防范和化解信息服务业务系统的安全风险,将风险控制在可接受的水平,为最大限度地保障信息服务业务系统的安全提供科学依据。

3.1.3

信息服务业务系统资产 Asset of Information Service System

电话: 82054513 http://www.ptsn.net.cn

YD/T 2243-2016

信息服务业务系统中具有价值的资源，是安全防护体系保护的主体。信息服务业务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，如局域网中的路由器。

3.1.4

信息服务业务系统资产价值 Asset value of Information Service System

信息服务业务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。

3.1.5

信息服务业务系统灾难 Disaster of Information Service System

由于各种原因，造成信息服务业务系统故障或瘫痪，使信息服务业务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。

3.1.6

信息服务业务系统灾难恢复 Disaster Recovery of Information Service System

为了将信息服务业务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。

3.2 缩略语

下列缩略语适用于本文件。

CPU	Central Processing Unit	中央处理器
DDoS	Distributed Denial of Service	分布式拒绝服务
DoS	Denial of Service	拒绝服务
IP	Internet Protocol	网际协议
MAC	Media Access Control	物理地址
SSL	Secure Sockets Layer	安全套接层
TLS	Transport Layer Security	安全传输层协议

4 信息服务业务系统安全防护概述

4.1 信息服务业务系统安全防护范围

信息服务业务是指通过信息采集、开发、处理和信息平台的建设，通过公众通信网络直接向终端用户提供语音信息服务（声讯服务）或在线信息和数据检索等信息服务的业务。信息服务的类型按照信息组织、传递等技术服务方式，主要包括但不限于信息发布平台和递送服务、信息搜索查询服务、信息社区服务、信息即时交互服务、信息保护和处理服务等。信息服务业务系统指向公众提供信息服务业务的系统或平台。

本标准主要对信息服务业务系统提出安全防护要求，如图 1 所示。为信息服务业务系统提供域名解析服务的系统的安全防护要求见 YD/T 2052-2009。与互联网相关的互联网数据中心见 YD/T 2584-2013，互联网内容分发网络见 YD/T 2589-2013。

电话：82054513 http://www.ptsn.net.cn

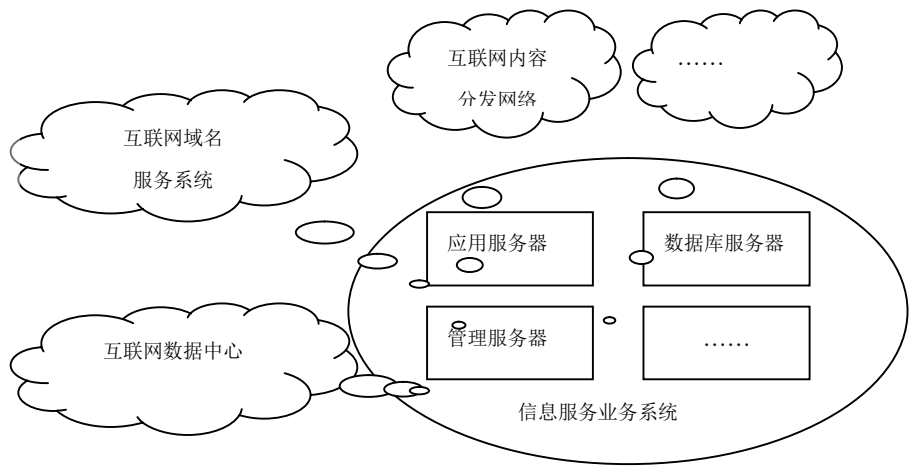


图 1 信息服务业务系统示意图

4.2 信息服务业务系统安全风险分析

信息服务业务系统的重要资产至少应包括：

- 信息服务业务系统相关设备及操作维护终端硬件及相关软件；
- 信息服务业务系统关键数据，如业务数据、系统配置数据、操作维护记录、用户信息等。

信息服务业务系统其他资产见附录 A 表 A.1 对资产的分类及举例。

信息服务业务系统的脆弱性可以从技术脆弱性和管理脆弱性两个方面考虑。脆弱性识别对象应以资产为核心。信息服务业务系统的脆弱性分析应包括但不限于附录 A 表 A.2 所列范围。

信息服务业务系统的威胁根据来源可分为技术威胁、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。信息服务业务系统的威胁分析应包括但不限于附录 A 表 A.3 所列范围。

信息服务业务系统可能存在的安全脆弱性被利用后会产生很大的安全风险，主要包含以下几个方面：

- 信息服务业务系统相关设备及操作维护终端硬件及相关软件：

信息服务业务系统相关设备及操作维护终端硬件及相关软件可能面临的安全风险主要包括：一是遭受 DDOS 攻击，导致系统中服务器或数据库等设备运行故障或宕机；二是系统被入侵，导致大量重要业务数据、系统配置数据、操作维护记录、用户信息的泄露，甚至系统瘫痪等。

- 信息服务业务系统关键数据：

信息服务业务系统关键数据可能面临的安全风险主要包括：系统升级或联网交互时感染包含病毒、木马、恶意链接等恶意代码，导致重要业务数据、系统配置数据、操作维护记录、用户信息被篡改或泄露，系统无法提供稳定的服务。

4.3 信息服务业务系统安全防护内容

信息服务业务系统主要为终端用户提供各类型的信息服务业务，因此保障业务的安全稳定运行和用户信息的安全可靠至关重要。保障信息服务业务系统基础设施的物理安全、管理安全等也是安全防护的主要内容。信息服务业务系统的安全防护内容具体包括：

- a) 业务及应用安全：业务及应用安全包括向用户提供的相关业务及应用在实现技术、逻辑、管理和控制等方面的安全要求，主要包括通用要求和特定业务相关要求。

电话：82054513 http://www.ptsn.net.cn

YD/T 2243-2016

b) 网络安全：网络安全主要包括信息服务业务系统内部网络结构安全、入侵防范和安全审计方面的安全防护要求。

c) 设备及软件系统安全：设备及软件系统安全主要包括网络及安全设备、操作系统、数据库、中间件在身份鉴别、访问控制、安全审计、入侵防范、资源控制等方面的安全防护要求。

d) 物理安全：物理安全主要包括系统所处的物理环境在机房位置、电力供应、防火、防水、防静电、温湿度控制等方面的安全防护要求。

e) 管理安全：管理安全主要包括管理制度、人员和技术支持能力、运行维护管理能力、灾难恢复预案等方面的安全防护要求。

5 信息服务业务系统安全防护要求

5.1 第 1 级要求

5.1.1 业务及应用安全

5.1.1.1 业务逻辑安全

5.1.1.1.1 身份鉴别

身份鉴别应符合以下要求：

- a) 对保留用户个人信息或用户服务信息的业务，应对登录用户进行身份标识和鉴别；
- b) 应采用加密方式存储业务用户的密码信息；
- c) 应提供并启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
- d) 应提供并启用户身份标识唯一检查功能，保证系统中不存在重复用户身份标识。在重要的功能操作中，再次验证用户的唯一标识，以规避越权漏洞。

5.1.1.1.2 访问控制

应由授权主体配置访问控制策略，并严格限制默认用户的访问权限。

5.1.2 网络安全

应绘制与当前运行情况相符的系统拓扑结构图。

5.1.3 设备及软件系统安全

5.1.1.2 网络及安全设备

应满足 YD/T 2698-2014 和 YD/T 2699-2014 的相关要求。

5.1.1.3 操作系统

应满足 YD/T 2701-2014 的相关要求。

5.1.1.4 数据库

应满足 YD/T 2700-2014 的相关要求。

5.1.1.5 中间件

应满足 YD/T 2702-2014 的相关要求。

5.1.4 物理安全

应满足 YD/T 1754-2008 中第 1 级的相关要求。

5.1.5 管理安全

应满足 YD/T 1756-2008 中第 1 级的相关要求。

5.2 第 2 级要求

5.2.1 业务及应用安全

5.2.1.1 业务逻辑安全

5.2.1.1.1 身份鉴别

除满足第1级的要求之外，还应满足：

- a) 应提供并启用用户鉴别信息复杂度检查功能，保证身份鉴别信息不易被冒用；
- b) 应严格设置登录策略，按安全策略要求具备防范账户暴力破解攻击措施的能力。如限定用户连续错误输入密码次数，超过设定阈值，对用户进行锁定，并设定锁定时间，在锁定时间内被锁定的用户需通过注册时的约定信息进行密码重新设定。

5.2.1.1.2 访问控制

除满足第1级的要求之外，还应严格限制各用户的访问权限，按安全策略要求控制用户对业务、数据、网络资源等的访问。

5.2.1.1.3 安全审计

安全审计应符合以下要求：

- a) 审计范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件。如普通用户异常登录、发布恶意代码、异常修改帐号信息等行为，以及管理员在业务功能及帐号控制方面的关键操作；
- b) 应保护审计记录，保证无法删除、修改或覆盖等；
- c) 业务相关审计记录应包括事件日期、时间、发起者信息、类型、描述和结果等；
- d) 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

5.2.1.1.4 资源控制

当用户和业务系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话。

5.2.1.1.5 灾难备份

灾难备份应符合以下要求：

- a) 应建立相关业务及应用系统的灾难恢复预案，并定期进行教育、培训和演练；
- b) 应建立对业务及应用关键数据（如重要业务数据、系统配置数据、操作维护记录、用户信息等）进行备份和恢复的管理和控制机制，并有必要的容灾备份。
- c) 相关数据备份范围和时间间隔、数据恢复能力应满足行业管理、业务运营企业应急预案相关要求。

5.2.1.2 Web 安全

5.2.1.2.1 输入验证

输入验证应符合以下要求：

- a) 应对所有来源的输入进行验证，按默认所有输入都可能包含恶意信息的原则进行安全检测，只要其来源不在可信任的范围之内，就应对输入来源进行验证；
- b) 用户身份标识和验证应在服务器端进行处理，避免在客户端进行的验证被绕过；
- c) 应对输入内容进行规范化处理后再进行验证，如文件路径、URL地址等；
- d) 应防止关键参数被篡改，关键参数应直接从服务器端读取，避免从客户端输入。

5.2.1.2.2 身份认证

身份认证应符合以下要求：

- a) 应禁止明文传输用户密码,可采用SSL加密隧道确保用户密码的传输安全;
- b) 应禁止在数据库或文件系统中明文存储用户密码,可采用单向散列值在数据库中存储用户密码,降低存储的用户密码被字典攻击的风险;
- c) 应禁止在COOKIE中保存用户密码;
- d) 当用户登录失败超过一定次数时,应采用图形验证码来增强身份认证安全,防止恶意脚本自动发送身份认证请求来猜测用户认证鉴权性质的信息,且图形验证码应能够抵抗工具的自动识别;
- e) 应对关键业务操作进行二次鉴权,例如修改用户认证鉴权信息(如密码、密码取回问题及答案、绑定手机号码等);
- f) 应避免认证错误提示泄露信息,在认证失败时,应向用户提供通用的错误提示信息,不应区分是帐号错误还是密码错误,避免这些错误提示信息被攻击者利用;
- g) 应支持密码策略设置,从业务系统层面支持强制的密码策略,包括密码长度、复杂度等,特别是业务系统的管理员密码;
- h) 应支持帐号锁定功能,系统应限制连续登录失败次数,在客户端多次尝试失败后,服务器端需要对用户帐号进行短时锁定,且锁定策略支持配置解锁时长。

5.2.1.2.3 访问控制

访问控制应符合以下要求:

- a) 应确保用户不能访问到未授权的功能和数据,未经授权的用户试图访问受限资源时,系统应以拒绝或提示用户进行身份鉴权;
- b) 应在服务器端实现对系统内受限资源的访问控制,避免客户端访问控制被绕过;
- c) 应采用统一的访问控制机制,保证整体访问控制策略的一致性。同时应确保访问控制策略不被非法修改。

5.2.1.2.4 会话管理

会话管理应符合以下要求:

- a) 应确保会话的安全创建,在用户认证成功后,应为用户创建新的会话并释放原有会话,创建的会话标识应满足随机性和长度要求,避免被攻击者猜测。
- b) 应确保会话数据的存储安全,用户登录成功后所生成的会话数据应存储在服务器端,并确保会话数据不能被非法访问,当更新会话数据时,要对数据进行严格的输入验证,以免会话数据的非法篡改。
- c) 应确保会话数据的传输安全,防止泄露会话标识。
- d) 应确保会话的安全终止,当用户登录成功并成功创建会话后,应在Web应用系统的各个页面提供用户登出功能,登出时应及时删除服务器端的会话数据。当处于登录状态的用户直接关闭浏览器时,需要提示用户执行安全登出或者自动为用户完成登出过程,从而安全的终止本次会话。
- e) 应设置合理的会话超时阈值,在合理范围内尽可能减小会话超时阈值,降低会话被劫持和重复攻击的风险,超过会话超时阈值后立刻销毁会话,清除会话的信息。
- f) 应限制系统会话并发连接数和同一用户的会话并发连接数,避免恶意用户创建多个并发的会话来消耗系统资源,影响业务可用性。

5.2.1.2.5 数据存储

数据存储应符合以下要求:

- a) 对于不同安全级别的数据,比如日志记录和业务数据,应采取相应的隔离措施和安全保护措施。

b) 应避免在代码中直接嵌入密码, 会导致密码修改困难, 甚至密码的泄露, 可从配置文件载入密码。

5.2.1.2.6 数据传输

应确保敏感信息通信信道的安全, 可在客户端与 Web 服务器之间使用 SSL, 使用 SSL 3.0/ TLS 1.0 以上版本, 对称加密密钥长度不少于 128 位, 非对称加密密钥长度不少于 1024 位, 单向散列值位数不小于 128 位。

5.2.1.2.7 日志记录

日志记录应符合以下要求:

a) 日志记录范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件。如普通用户异常登录、发布恶意代码、异常修改帐号信息等行为, 以及管理员在业务功能及帐号控制方面的关键操作。

b) 应禁止在日志中记录用户密码, 验证授权标识等敏感信息。

c) 应防止日志欺骗, 如果在生成日志时需要引入来自非受信源的数据, 则需要严格校验, 防止日志欺骗攻击。

d) 应禁止将日志保存到 Web 目录下, 确保日志数据的安全存储并严格限制日志数据的访问权限, 可对日志记录进行签名来实现防篡改。

5.2.1.3 特定业务相关要求

门户综合网站业务系统、即时通信业务系统、搜索系统、信息社区服务系统的特定安全防护要求见附录 B、附录 C、附录 D、附录 E。

5.2.2 网络安全

5.2.2.1 结构安全

除满足第 1 级的要求之外, 还应满足:

a) 应根据应用和服务的特点, 在满足高峰期流量需求的基础上, 合理设计带宽。

b) 应根据系统内部网络结构特点, 按照统一的管理和控制原则划分不同的子网或网段, 设备依照功能及其重要性等因素分区部署。

c) 网络节点、链路应有足够冗余, 应能对主要网络设备进行状态监控。

d) 应避免将重要网段部署在网络边界处且直接连接外部信息系统, 重要网段与其他网段之间采取可靠的技术隔离手段。

e) 不考虑主动宕机维护的情况, 系统年宕机时间不超过 8.76 小时, 可靠性应达到 99.9% 以上。

5.2.2.2 入侵防范

除满足第 1 级的要求之外, 还应满足:

a) 应在系统边界处监视以下攻击行为: 端口扫描、强力攻击、木马后门攻击、DoS/DDoS 攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等。

b) 应在系统边界处部署防火墙等安全防御设备或技术措施, 有效抵御和防范各种攻击。

5.2.2.3 安全监测

除满足第 1 级的要求之外, 还应满足:

a) 应对系统边界流量进行 DDoS 攻击监测, 发现攻击行为在 60s 之内提供告警, 并进行相应处置。

b) 应定期（至少每半个月）对木马后门攻击、缓冲区溢出攻击和网络蠕虫攻击等进行检测，发现攻击行为在60s之内提供告警，并进行相应处置。

c) 应对系统中的重要设备运行状况进行监测，发现异常情况（如系统宕机等）在20s之内提供告警，并进行相应处置。

d) 应对系统中的网络流量信息进行监测，发现异常情况（如达到网络链路容量的三分之二及以上）在60s之内提供告警，并进行相应处置。

e) 应对系统中的各类监测数据进行日志记录，并且保留一定期限（至少180天）。

5.2.2.4 安全审计

除满足第1级的要求之外，还应满足：

a) 审计记录应包括事件的日期、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。

b) 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

c) 应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。

5.2.3 设备及软件系统安全

5.2.3.1 网络及安全设备

除满足第1级要求之外，还应满足：

a) 应保证主要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。

b) 关键网络设备、重要线路、网络设备的重要部件应采用冗余的保护方式。

5.2.3.2 操作系统

除满足第1级要求之外，还应满足：

5.2.3.2.1 安全审计

安全审计应符合以下要求：

a) 审计范围应覆盖到主机/服务器上的每个操作系统用户。

b) 审计内容应包括重要操作维护用户行为、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相关事件。

c) 审计记录应包括事件的日期、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等。

d) 应保护审计记录，避免其受到未预期的删除、修改或覆盖等，保留一定期限（至少180天）。

5.2.3.2.2 灾难备份

应建立对主机关键数据（如主机配置数据、管理员操作维护记录、用户信息等）和重要信息进行备份和恢复的管理和控制机制，相关主机数据备份范围和时间间隔、数据恢复能力应满足行业管理、业务运营企业应急预案相关要求。

5.2.3.3 数据库

同第1级要求。

5.2.3.4 中间件

应对 Web 中间件、Web 第三方插件和框架的默认口令进行修改，并具有复杂度要求。

5.2.4 物理安全

应满足 YD/T 1754-2008 中第2级的相关要求。

5.2.5 管理安全

除满足 YD/T 1756-2008 中第 2 级的相关要求之外，还应满足：

- a) 信息服务业务系统及其所属各类设备应按照 YD/T 1730-2008 的相关要求定期进行安全风险评估（至少每两年一次），风险评估范围应与信息服务业务系统安全防护范围一致。
- b) 信息服务业务系统安全风险评估至少应覆盖业务及应用安全、网络安全、设备及软件系统安全、物理环境安全等相关技术风险和人员安全、运维安全等相关管理风险，至少包含信息服务业务系统相关资产、脆弱性、威胁、安全措施、风险分析等要素和内容，并根据评估结果制定相应的风险处理计划。
- c) 信息服务业务系统应按照 YD/T 1731-2008 的相关要求制定灾难恢复预案，并定期组织灾难恢复预案的教育培训（至少每半年一次）和演练（至少每年一次）。

5.3 第 3 级要求

5.3.1 业务及应用安全

5.3.1.1 业务逻辑安全

除满足第 2 级的要求之外，还应满足：

- a) 应能防止身份鉴别暴力攻击（如登录模块随机验证码验证、并且保证验证码不易被自动预测、识别）；
- b) 加强口令复杂度要求，不应含有常用字符组合、数字组合、键盘顺序等可预测密码组合；
- c) 应能根据需要对业务及应用相关通信过程中的全部报文或整个会话过程提供必要的保护（如进行通信数据加密），并提供业务及应用相关访问、通信等数据的防抵赖功能；
- d) 应定义业务水平阈值，能够对业务及应用服务水平进行检测，并具备当服务水平降低到预先规定的阈值时进行告警的功能；
- e) 应对业务用户访问和操作的有关环节（如注册、登录、操作、管理、浏览等）提供有效的保护措施（如用户注册口令进行强度检查、用户 ID 检测和帐号保护、以图形验证码保护各类提交信息、对用户重要操作进行确认和验证、授权访问页面使用安全连接等）；
- f) 提供重要服务的业务及应用系统应进行系统级备份，以保证其业务连续性；
- g) 重要服务的业务及应用相关数据应进行异址备份；
- h) 应提供数据自动保护功能，当发生故障后应保证系统能够恢复到故障前的业务状态。

5.3.1.2 Web 安全

除满足第 2 级的要求之外，还应满足：

- a) 在涉及到关键业务操作的 Web 页面，应为当前 Web 页面生成一次性随机令牌，作为主会话标识的补充。在执行关键业务前，应确保用户提交的一次性随机令牌与服务器端保存的一次性随机令牌匹配，以避免跨站请求伪造等攻击。
- b) Web 程序上线前或升级后应进行代码审计，形成报告，并对审计发现的问题进行代码升级完善；
- c) 应避免使用含有已公开漏洞的开源第三方应用组件及代码（漏洞库可参考 CVE、CNVD 等）。

5.3.1.3 特定业务相关要求

门户综合网站业务系统、即时通信业务系统、搜索系统、信息社区服务系统的特定安全防护要求见附录 B、附录 C、附录 D、附录 E。

5.3.2 网络安全

5.3.2.1 结构安全

除满足第 2 级的要求之外，还应满足：

- a) 系统应具有过负荷保护功能，确保系统在过负荷时，重要业务能正常运行；
- b) 应具备必要的流量负荷分担设计；
- c) 不考虑主动宕机维护的情况，系统年宕机时间不超过4.38小时，可靠性应达到99.95%以上；
- d) 应能采取有效手段（如IP地址与MAC地址绑定等）防止地址欺骗及嗅探攻击。

5.3.2.2 安全监测

除满足第2级的要求之外，还应满足：

- a) 应对重要服务器进行入侵行为监测，能够记录入侵的源IP、攻击的类型、攻击的目的地址、攻击的时间，发现严重入侵事件在60s之内提供告警，并进行相应处置。
- b) 应对重要服务器进行性能监测，包括服务器的CPU、硬盘、内存、网络等资源的使用情况，发现异常情况（如达到资源容量的三分之二及以上）在60s之内提供告警，并进行相应处置。
- c) 应对服务器、数据库等系统的服务水平设定告警阈值并进行监测，发现服务水平降低到阈值时在60s之内提供告警，并进行相应处置。

5.3.3 设备及软件系统安全

5.3.3.1 网络及安全设备

除满足第2级的要求之外，还应满足：

- a) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。
- b) 设备应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵时优先保护重要主机。
- c) 应定期自检（漏洞扫描、弱口令扫描、基线配置信息等），对设备的端口、弱口令、安全漏洞、木马等进行扫描。
- d) 重要设备、线路应采用热备份的保护方式进行保护。

5.3.3.2 操作系统

除满足第2级的要求之外，还应满足：

5.3.3.2.1 身份鉴别

身份鉴别应符合以下要求：

- a) 应采用两种或两种以上组合的鉴别技术对相关设备的管理用户进行身份鉴别。
- b) 重要主机应使用安全性较高的身份鉴别措施（如数字证书等）对用户进行身份鉴别。

5.3.3.2.2 安全审计

安全审计应符合以下要求：

- a) 应能根据记录数据进行分析，并生成审计报告。
- b) 应保护审计进程，避免受到未预期的中断。

5.3.3.2.3 灾难备份

灾难备份应符合以下要求：

- a) 系统应具备较好的灾难备份和业务恢复能力，提供重要服务的业务及应用系统应进行系统级备份，以保证业务的连续性。
- b) 应提供数据自动保护功能，当发生故障后应保证系统能够恢复到故障前的业务状态，重要的数据应进行异地备份。

5.3.3.3 数据库

同第 2 级要求。

5.3.3.4 中间件

同第 2 级要求。

5.3.4 物理安全

应满足 YD/T 1754-2008 中第 3.1 级的相关要求。

5.3.5 管理安全

除应满足第 2 级要求和 YD/T 1756-2008 中第 3.1 级的相关要求之外，还应满足：

- a) 应定期对信息服务业务系统及其所属各类设备进行安全风险评估（至少每年一次）。
- b) 信息服务业务系统灾难恢复预案应按照安全管理制度相关的制修订要求进行管理。

5.4 第 4 级要求

待定。

5.5 第 5 级要求

待定。

附 录 A (规范性附录)

信息服务业务系统风险分析

本附录指导信息服务业务系统风险分析过程中的资产、脆弱性、威胁分析。

信息服务业务系统的资产至少应包括：设备软硬件，重要数据，文档，人员等，如表 A.1 所示。

表 A.1 资产列表

类别	主要资产
设备及链路	各类业务及应用涉及的操作维护终端、服务器和数据库，各类业务及应用相关辅助设备（如安全过滤、入侵检测和防护设备），系统内部网络设备（如系统内部组网路由器、交换机等设备）、系统内部链路
软件	相关业务或应用软件、数据库软件、业务控制和运维管理软件等
数据和信息	保证业务正常提供的数据和信息（如业务数据、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	系统提供的相关业务和应用
文档和资料	纸质以及保存在存储介质中的各种文件资料（如设计文档、技术要求、管理规定、工作计划、技术报告、用户手册等）
人员	相关管理、维护、开发、数据备份人员等
环境和设施	业务系统和设备所处的物理环境，机房、电力、防火、防水、防静电、温湿度控制等相关设施

表 A.2 列举出信息服务业务系统的主要的脆弱性识别内容。

表 A.2 脆弱性分析表

类别	对象	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，访问控制策略设置不合理； 相关服务器的日志功能没有启用或不够详细； 系统规划、设备部署、链路部署、资源配置、业务保护和恢复能力、安全技术措施和策略等方面的缺陷
	设备	相关设备存在硬件隐患或质量问题； 相关设备的操作系统存在安全隐患； 相关密码设置不合理、复杂度不够、或没有经常更新； 设备重要部件未进行合理备份； 相关设备超过使用年限或核心部件老化； 相关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、主机等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

信息服务业务系统安全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 A.3 列举出信息服务业务系统主要面临的威胁。

表 A.3 威胁来源列表

类别		主要威胁
技术威胁		相关主机和服务器、及系统网络设备使用时间过长或质量问题等导致硬件故障； 系统链路发生故障； 相关设备的操作系统软件、应用软件运行故障； 相关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； 意外事故或通讯线路方面的故障
	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
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
	非恶意人员	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

附录 B
(规范性附录)

门户综合网站业务系统特定安全防护要求

B.1 第 1 级要求

应根据用户需求递送相关信息内容，支持用户对递送信息的退订。
应建立相关机制清除已发现的有害信息。

B.2 第 2 级要求

除满足第 1 级的要求之外，还应满足：

- a) 不应向公众发布有害信息，应对通过该平台对外发布的公共信息使用自动程序过滤和人工检查结合的方式进行有害信息检查、屏蔽和删除，防止有害信息通过业务网络向公众传播；
- b) 应对含有恶意代码链接的信息建立发现和处理机制，防止类似信息的扩散；
- c) 应记录用户发布信息、评论等相关日志信息（如操作内容、操作时间、使用的网络地址或者域名等），并且保留一定期限（至少60天）；
- d) 应确保不非法操作与自身功能不相关的文件；
- e) 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和插件。

B.3 第 3 级要求

除满足第 2 级的要求之外，还应满足：

- a) 应提供有效的恶意代码检测和过滤技术手段，对业务平台向用户提供的各类信息（如用户发布和上传的文件、资源站点可供下载的文件等）进行必要的安全检查和过滤；
- b) 应拒绝由未被允许的地址、子网域发起的请求（如浏览、发布、评论等），应拒绝以未经授权的方式访问服务器上有限公开的相关内容和资源；
- c) 提供下载服务的平台，应能拒绝来自未被允许的地址、用户名、子网域的操作请求，有效保护或隔离核心服务器相关资源；
- d) 提供下载服务的平台，应能限制单个地址（地址段）、用户名、子网域的连接数量和连接频率，防止资源被过度使用；
- e) 应能根据相关内容（如静态信息、流媒体等）的特点提供差异化的业务质量控制和管理策略，根据平台内、外部性能监测的状况，实时智能的平衡和优化网络流量。

B.4 第 4 级要求

待定。

B.5 第 5 级要求

待定。

附 录 C

(规范性附录)

即时通信业务系统特定安全防护要求

C.1 第 1 级要求

应提供相关控制机制，由用户决定是否同意接收推送提示消息、添加新通信对象，建立新会话等，防止恶意骚扰。

未经用户同意，不得擅自为用户自动开启其他服务功能（如定位功能等）。

C.2 第 2 级要求

除满足第 1 级的要求之外，还应满足：

- a) 对以群发方式发送的伪造、隐匿信息发送者真实标记的即时消息，应能够防范、清除；
- b) 应确保不非法操作与自身功能不相关的文件；
- c) 应禁止不必要的内嵌网络服务，禁止在用户端自动安装恶意软件和插件；
- d) 应对用户间的通信数据进行检查，当发现恶意信息时对用户进行及时提醒告警，如恶意链接等。

C.3 第 3 级要求

除满足第 2 级的要求之外，还应满足：

- a) 应提供必要的保护措施（如加密机制）保护用户间通信数据的机密性和完整性；
- b) 应对用户上传、下载等操作行为进行监控，防止用户的非授权读写操作；
- c) 应提供有效的恶意代码检测和过滤技术手段，对业务平台向用户提供的各类信息（如即时通信用户间传送的文件等）进行必要的安全检查和过滤；
- d) 应对存储于服务器的用户通信信息提供必要的保护，防止被窃取或篡改。

C.4 第 4 级要求

待定。

C.5 第 5 级要求

待定。

附 录 D

(规范性附录)

搜索系统特定安全防护要求

D.1 第 1 级要求

应及时清除搜索结果中存在恶意信息的条目。

D.2 第 2 级要求

除满足第1级的要求之外，还应满足：

- a) 应对含有恶意代码链接的信息建立发现和处理机制，防止类似信息的扩散；
- b) 应确保不非法操作与自身功能不相关的文件；
- c) 应禁止不必要的内嵌网络服务，禁止在用户端自动安装恶意软件和插件；
- d) 不应向公众提供含有有害信息的访问链接，应使用自动程序过滤和人工检查结合的方式进行有害信息检查、屏蔽和删除，防止有害信息通过搜索服务向公众传播；
- e) 应建立相关机制保护用户搜索操作等相关日志信息（如搜索内容、搜索时间、访问的网络地址或者域名等）。

D.3 第 3 级要求

除满足第2级的要求之外，还应满足：

- a) 应对输入数据做严格验证，默认所有输入都可能包含恶意信息；
- b) 应能限制单个地址（地址段）、子网域的连接数量和连接频率，防止资源被过度使用；
- c) 应对可能存在恶意信息的条目进行标注并提醒用户，保障用户的安全。

D.4 第 4 级要求

待定。

D.5 第 5 级要求

待定。

附录 E

(规范性附录)

信息社区服务系统的特定安全防护要求

E.1 第 1 级要求

应根据用户需求递送相关信息内容，支持用户对信息的退订。

未经用户同意，不得擅自为用户自动开启其他服务功能（如定位功能等）。

E.2 第 2 级要求

除满足第1级的要求之外，还应满足：

- a) 应能对含有恶意代码链接的信息建立发现和处理机制，防止类似信息的扩散；
- b) 应记录用户发布信息、评论、文件上传和下载等相关日志信息（如操作内容、操作时间、使用的网络地址或者域名等），并且保留一定期限（至少60天）；
- c) 应确保不非法操作与自身功能不相关的文件；
- d) 应禁止不必要的内嵌网络服务，禁止在用户端自动安装恶意软件和插件。

E.3 第 3 级要求

除满足第2级的要求之外，还应满足：

- a) 应提供有效的恶意代码检测和过滤技术手段，对业务平台向用户提供的各类信息（如用户发布和上传的文件等）进行必要的安全检查和过滤；
- b) 应对输入数据做严格验证，默认所有输入都可能包含恶意信息；
- c) 应对用户上传、下载等操作行为进行监控，防止用户的非授权读写操作；
- d) 应拒绝由未被允许的地址、子网域发起的请求（如浏览、发布、评论等），拒绝以未经授权的方式访问有限公开的内容和资源；
- e) 应能限制单个地址（地址段）、用户名、子网域的连接数量和连接频率，防止资源被过度使用；
- f) 应能根据相关内容（如静态信息、流媒体等）的特点提供差异化的业务质量控制和管理策略，根据平台内、外部性能监测的状况，实时智能的平衡和优化网络流量。

E.4 第 4 级要求

待定。

E.5 第 5 级要求

待定。

参 考 文 献

- [1] GB 17859-1999 计算机信息系统安全等级划分准则
 - [2] GB/T 18336-2000 信息技术信息技术安全性评估准则
 - [3] GB/T 19716-2005 信息技术信息安全管理实用规则
 - [4] GB/T 19715.2-2005 信息技术信息安全管理指南第 2 部分
 - [5] GB/T 22239-2008 信息安全技术信息系统安全等级保护基本要求
 - [6] 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
-