

ICS 35.110

M 11

YD

中华人民共和国通信行业标准

YD/T 1736-2009

代替 YD/T 1736-2008

互联网安全防护要求

Security protection requirements for internet

2009-12-11 发布

2010-01-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言.....II

1 范围.....1

2 规范性引用文件.....1

3 术语和定义.....1

4 缩略语.....3

5 互联网安全防护概述.....3

 5.1 互联网安全防护范围.....3

 5.2 互联网安全防护内容.....4

6 互联网定级对象和安全等级确定.....4

7 互联网资产、脆弱性、威胁分析.....5

 7.1 资产分析.....5

 7.2 脆弱性分析.....5

 7.3 威胁分析.....6

8 互联网安全等级保护要求.....7

 8.1 第 1 级要求.....7

 8.2 第 2 级要求.....7

 8.3 第 3.1 级要求.....11

 8.4 第 3.2 级要求.....14

 8.5 第 4 级要求.....14

 8.6 第 5 级要求.....14

9 互联网灾难备份及恢复要求.....14

 9.1 互联网灾难备份及恢复等级要求.....14

 9.2 第 1 级要求.....14

 9.3 第 2 级要求.....14

 9.4 第 3.1 级要求.....15

 9.5 第 3.2 级要求.....16

 9.6 第 4 级要求.....16

 9.7 第 5 级要求.....16

参考文献.....17

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》（本标准）
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》

本标准与YD/T 1737-2009《互联网安全防护检测要求》（修订YD/T 1737-2008《互联网安全防护检测要求》）配套使用。

本标准是YD/T 1736-2008《互联网安全防护要求》的修订版本。本标准与YD/T 1736-2008的主要差异在于：

1. 本标准的第2章“规范性引用文件”中补充和更新了标准正文中引用的规范文件。
2. 本标准的第4章“缩略语”中补充和更新了标准正文中适用的缩略语。
3. 本标准的第5章“互联网安全防护概述”中增加了“互联网安全等级保护”相关“业务及应用系统安全”要求的内容和说明。
4. 本标准的第7章“互联网资产、脆弱性、威胁分析”中增加了“环境和设施”类资产及其主要资产说明。
5. 本标准的第8章“互联网安全等级保护要求”中修改和补充了安全等级保护相关要求和内容，主要涉及8.2节、8.3节。其中，“业务及应用安全要求”部分增加了“互联网虚拟专用网服务”相关内容，主要涉及8.2.1.6节、8.3.1.6节；增加了“业务及应用系统安全要求”相关内容，主要涉及8.2.2节、8.3.2节；修改了“设备安全要求”相关内容，主要涉及8.2.3.2节、8.3.3.2节；增加了“物理环境安全要求”的相关内容，主要涉及8.2.4节、8.3.4节；删除了“移动互联网信息服务安全要求”相关内容，主要涉及原8.2.1.7节、原8.3.1.7节。

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、中国电信集团公司、中国移动通信集团公司、中国联通网络通信集团有限公司。

本标准主要起草人：杨剑锋、杨洋、田慧蓉、赵阳、刘楠、李金玉、杜之亨、张云勇。

本标准于2008年1月首次发布，本次为第一次修订。

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》

本标准与YD/T 1737-2009《互联网安全防护检测要求》（修订YD/T 1737-2008《互联网安全防护检测要求》）配套使用。

本标准是YD/T 1736-2008《互联网安全防护要求》的修订版本。本标准与YD/T 1736-2008的主要差异在于：

1. 本标准的第2章“规范性引用文件”中补充和更新了标准正文中引用的规范文件。
2. 本标准的第4章“缩略语”中补充和更新了标准正文中适用的缩略语。
3. 本标准的第5章“互联网安全防护概述”中增加了“互联网安全等级保护”相关“业务及应用系统安全”要求的内容和说明。
4. 本标准的第7章“互联网资产、脆弱性、威胁分析”中增加了“环境和设施”类资产及其主要资产说明。
5. 本标准的第8章“互联网安全等级保护要求”中修改和补充了安全等级保护相关要求和内容，主要涉及8.2节、8.3节。其中，“业务及应用安全要求”部分增加了“互联网虚拟专用网服务”相关内容，主要涉及8.2.1.6节、8.3.1.6节；增加了“业务及应用系统安全要求”相关内容，主要涉及8.2.2节、8.3.2节；修改了“设备安全要求”相关内容，主要涉及8.2.3.2节、8.3.3.2节；增加了“物理环境安全要求”的相关内容，主要涉及8.2.4节、8.3.4节；删除了“移动互联网信息服务安全要求”相关内容，主要涉及原8.2.1.7节、原8.3.1.7节。

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、中国电信集团公司、中国移动通信集团公司、中国联通网络通信集团有限公司。

本标准主要起草人：杨剑锋、杨洋、田慧蓉、赵阳、刘楠、李金玉、杜之亨、张云勇。

本标准于2008年1月首次发布，本次为第一次修订。

- 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》

本标准与YD/T 1737-2009《互联网安全防护检测要求》（修订YD/T 1737-2008《互联网安全防护检测要求》）配套使用。

本标准是YD/T 1736-2008《互联网安全防护要求》的修订版本。本标准与YD/T 1736-2008的主要差异在于：

- 1. 本标准的第2章“规范性引用文件”中补充和更新了标准正文中引用的规范文件。
- 2. 本标准的第4章“缩略语”中补充和更新了标准正文中适用的缩略语。
- 3. 本标准的第5章“互联网安全防护概述”中增加了“互联网安全等级保护”相关“业务及应用系统安全”要求的内容和说明。
- 4. 本标准的第7章“互联网资产、脆弱性、威胁分析”中增加了“环境和设施”类资产及其主要资产说明。
- 5. 本标准的第8章“互联网安全等级保护要求”中修改和补充了安全等级保护相关要求和内容，主要涉及8.2节、8.3节。其中，“业务及应用安全要求”部分增加了“互联网虚拟专用网服务”相关内容，主要涉及8.2.1.6节、8.3.1.6节；增加了“业务及应用系统安全要求”相关内容，主要涉及8.2.2节、8.3.2节；修改了“设备安全要求”相关内容，主要涉及8.2.3.2节、8.3.3.2节；增加了“物理环境安全要求”的相关内容，主要涉及8.2.4节、8.3.4节；删除了“移动互联网信息服务安全要求”相关内容，主要涉及原8.2.1.7节、原8.3.1.7节。

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、中国电信集团公司、中国移动通信集团公司、中国联通网络通信集团有限公司。

本标准主要起草人：杨剑锋、杨洋、田慧蓉、赵阳、刘楠、李金玉、杜之亨、张云勇。

本标准于2008年1月首次发布，本次为第一次修订。

- 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》

本标准与YD/T 1737-2009《互联网安全防护检测要求》（修订YD/T 1737-2008《互联网安全防护检测要求》）配套使用。

本标准是YD/T 1736-2008《互联网安全防护要求》的修订版本。本标准与YD/T 1736-2008的主要差异在于：

- 1. 本标准的第2章“规范性引用文件”中补充和更新了标准正文中引用的规范文件。
- 2. 本标准的第4章“缩略语”中补充和更新了标准正文中适用的缩略语。
- 3. 本标准的第5章“互联网安全防护概述”中增加了“互联网安全等级保护”相关“业务及应用系统安全”要求的内容和说明。
- 4. 本标准的第7章“互联网资产、脆弱性、威胁分析”中增加了“环境和设施”类资产及其主要资产说明。
- 5. 本标准的第8章“互联网安全等级保护要求”中修改和补充了安全等级保护相关要求和内容，主要涉及8.2节、8.3节。其中，“业务及应用安全要求”部分增加了“互联网虚拟专用网服务”相关内容，主要涉及8.2.1.6节、8.3.1.6节；增加了“业务及应用系统安全要求”相关内容，主要涉及8.2.2节、8.3.2节；修改了“设备安全要求”相关内容，主要涉及8.2.3.2节、8.3.3.2节；增加了“物理环境安全要求”的相关内容，主要涉及8.2.4节、8.3.4节；删除了“移动互联网信息服务安全要求”相关内容，主要涉及原8.2.1.7节、原8.3.1.7节。

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、中国电信集团公司、中国移动通信集团公司、中国联通网络通信集团有限公司。

本标准主要起草人：杨剑锋、杨洋、田慧蓉、赵阳、刘楠、李金玉、杜之亨、张云勇。

本标准于2008年1月首次发布，本次为第一次修订。

- 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》

本标准与YD/T 1737-2009《互联网安全防护检测要求》（修订YD/T 1737-2008《互联网安全防护检测要求》）配套使用。

本标准是YD/T 1736-2008《互联网安全防护要求》的修订版本。本标准与YD/T 1736-2008的主要差异在于：

- 1. 本标准的第2章“规范性引用文件”中补充和更新了标准正文中引用的规范文件。
- 2. 本标准的第4章“缩略语”中补充和更新了标准正文中适用的缩略语。
- 3. 本标准的第5章“互联网安全防护概述”中增加了“互联网安全等级保护”相关“业务及应用系统安全”要求的内容和说明。
- 4. 本标准的第7章“互联网资产、脆弱性、威胁分析”中增加了“环境和设施”类资产及其主要资产说明。
- 5. 本标准的第8章“互联网安全等级保护要求”中修改和补充了安全等级保护相关要求和内容，主要涉及8.2节、8.3节。其中，“业务及应用安全要求”部分增加了“互联网虚拟专用网服务”相关内容，主要涉及8.2.1.6节、8.3.1.6节；增加了“业务及应用系统安全要求”相关内容，主要涉及8.2.2节、8.3.2节；修改了“设备安全要求”相关内容，主要涉及8.2.3.2节、8.3.3.2节；增加了“物理环境安全要求”的相关内容，主要涉及8.2.4节、8.3.4节；删除了“移动互联网信息服务安全要求”相关内容，主要涉及原8.2.1.7节、原8.3.1.7节。

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、中国电信集团公司、中国移动通信集团公司、中国联通网络通信集团有限公司。

本标准主要起草人：杨剑锋、杨洋、田慧蓉、赵阳、刘楠、李金玉、杜之亨、张云勇。

本标准于2008年1月首次发布，本次为第一次修订。

- 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》

本标准与YD/T 1737-2009《互联网安全防护检测要求》（修订YD/T 1737-2008《互联网安全防护检测要求》）配套使用。

本标准是YD/T 1736-2008《互联网安全防护要求》的修订版本。本标准与YD/T 1736-2008的主要差异在于：

- 1. 本标准的第2章“规范性引用文件”中补充和更新了标准正文中引用的规范文件。
- 2. 本标准的第4章“缩略语”中补充和更新了标准正文中适用的缩略语。
- 3. 本标准的第5章“互联网安全防护概述”中增加了“互联网安全等级保护”相关“业务及应用系统安全”要求的内容和说明。
- 4. 本标准的第7章“互联网资产、脆弱性、威胁分析”中增加了“环境和设施”类资产及其主要资产说明。
- 5. 本标准的第8章“互联网安全等级保护要求”中修改和补充了安全等级保护相关要求和内容，主要涉及8.2节、8.3节。其中，“业务及应用安全要求”部分增加了“互联网虚拟专用网服务”相关内容，主要涉及8.2.1.6节、8.3.1.6节；增加了“业务及应用系统安全要求”相关内容，主要涉及8.2.2节、8.3.2节；修改了“设备安全要求”相关内容，主要涉及8.2.3.2节、8.3.3.2节；增加了“物理环境安全要求”的相关内容，主要涉及8.2.4节、8.3.4节；删除了“移动互联网信息服务安全要求”相关内容，主要涉及原8.2.1.7节、原8.3.1.7节。

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、中国电信集团公司、中国移动通信集团公司、中国联通网络通信集团有限公司。

本标准主要起草人：杨剑锋、杨洋、田慧蓉、赵阳、刘楠、李金玉、杜之亨、张云勇。

本标准于2008年1月首次发布，本次为第一次修订。

- 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》

本标准与YD/T 1737-2009《互联网安全防护检测要求》（修订YD/T 1737-2008《互联网安全防护检测要求》）配套使用。

本标准是YD/T 1736-2008《互联网安全防护要求》的修订版本。本标准与YD/T 1736-2008的主要差异在于：

- 1. 本标准的第2章“规范性引用文件”中补充和更新了标准正文中引用的规范文件。
- 2. 本标准的第4章“缩略语”中补充和更新了标准正文中适用的缩略语。
- 3. 本标准的第5章“互联网安全防护概述”中增加了“互联网安全等级保护”相关“业务及应用系统安全”要求的内容和说明。
- 4. 本标准的第7章“互联网资产、脆弱性、威胁分析”中增加了“环境和设施”类资产及其主要资产说明。
- 5. 本标准的第8章“互联网安全等级保护要求”中修改和补充了安全等级保护相关要求和内容，主要涉及8.2节、8.3节。其中，“业务及应用安全要求”部分增加了“互联网虚拟专用网服务”相关内容，主要涉及8.2.1.6节、8.3.1.6节；增加了“业务及应用系统安全要求”相关内容，主要涉及8.2.2节、8.3.2节；修改了“设备安全要求”相关内容，主要涉及8.2.3.2节、8.3.3.2节；增加了“物理环境安全要求”的相关内容，主要涉及8.2.4节、8.3.4节；删除了“移动互联网信息服务安全要求”相关内容，主要涉及原8.2.1.7节、原8.3.1.7节。

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、中国电信集团公司、中国移动通信集团公司、中国联通网络通信集团有限公司。

本标准主要起草人：杨剑锋、杨洋、田慧蓉、赵阳、刘楠、李金玉、杜之亨、张云勇。

本标准于2008年1月首次发布，本次为第一次修订。

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》

本标准与YD/T 1737-2009《互联网安全防护检测要求》（修订YD/T 1737-2008《互联网安全防护检测要求》）配套使用。

本标准是YD/T 1736-2008《互联网安全防护要求》的修订版本。本标准与YD/T 1736-2008的主要差异在于：

1. 本标准的第2章“规范性引用文件”中补充和更新了标准正文中引用的规范文件。
2. 本标准的第4章“缩略语”中补充和更新了标准正文中适用的缩略语。
3. 本标准的第5章“互联网安全防护概述”中增加了“互联网安全等级保护”相关“业务及应用系统安全”要求的内容和说明。
4. 本标准的第7章“互联网资产、脆弱性、威胁分析”中增加了“环境和设施”类资产及其主要资产说明。
5. 本标准的第8章“互联网安全等级保护要求”中修改和补充了安全等级保护相关要求和内容，主要涉及8.2节、8.3节。其中，“业务及应用安全要求”部分增加了“互联网虚拟专用网服务”相关内容，主要涉及8.2.1.6节、8.3.1.6节；增加了“业务及应用系统安全要求”相关内容，主要涉及8.2.2节、8.3.2节；修改了“设备安全要求”相关内容，主要涉及8.2.3.2节、8.3.3.2节；增加了“物理环境安全要求”的相关内容，主要涉及8.2.4节、8.3.4节；删除了“移动互联网信息服务安全要求”相关内容，主要涉及原8.2.1.7节、原8.3.1.7节。

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、中国电信集团公司、中国移动通信集团公司、中国联通网络通信集团有限公司。

本标准主要起草人：杨剑锋、杨洋、田慧蓉、赵阳、刘楠、李金玉、杜之亨、张云勇。

本标准于2008年1月首次发布，本次为第一次修订。

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》

本标准与YD/T 1737-2009《互联网安全防护检测要求》（修订YD/T 1737-2008《互联网安全防护检测要求》）配套使用。

本标准是YD/T 1736-2008《互联网安全防护要求》的修订版本。本标准与YD/T 1736-2008的主要差异在于：

1. 本标准的第2章“规范性引用文件”中补充和更新了标准正文中引用的规范文件。
2. 本标准的第4章“缩略语”中补充和更新了标准正文中适用的缩略语。
3. 本标准的第5章“互联网安全防护概述”中增加了“互联网安全等级保护”相关“业务及应用系统安全”要求的内容和说明。
4. 本标准的第7章“互联网资产、脆弱性、威胁分析”中增加了“环境和设施”类资产及其主要资产说明。
5. 本标准的第8章“互联网安全等级保护要求”中修改和补充了安全等级保护相关要求和内容，主要涉及8.2节、8.3节。其中，“业务及应用安全要求”部分增加了“互联网虚拟专用网服务”相关内容，主要涉及8.2.1.6节、8.3.1.6节；增加了“业务及应用系统安全要求”相关内容，主要涉及8.2.2节、8.3.2节；修改了“设备安全要求”相关内容，主要涉及8.2.3.2节、8.3.3.2节；增加了“物理环境安全要求”的相关内容，主要涉及8.2.4节、8.3.4节；删除了“移动互联网信息服务安全要求”相关内容，主要涉及原8.2.1.7节、原8.3.1.7节。

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、中国电信集团公司、中国移动通信集团公司、中国联通网络通信集团有限公司。

本标准主要起草人：杨剑锋、杨洋、田慧蓉、赵阳、刘楠、李金玉、杜之亨、张云勇。

本标准于2008年1月首次发布，本次为第一次修订。

- 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》

本标准与YD/T 1737-2009《互联网安全防护检测要求》（修订YD/T 1737-2008《互联网安全防护检测要求》）配套使用。

本标准是YD/T 1736-2008《互联网安全防护要求》的修订版本。本标准与YD/T 1736-2008的主要差异在于：

- 1. 本标准的第2章“规范性引用文件”中补充和更新了标准正文中引用的规范文件。
- 2. 本标准的第4章“缩略语”中补充和更新了标准正文中适用的缩略语。
- 3. 本标准的第5章“互联网安全防护概述”中增加了“互联网安全等级保护”相关“业务及应用系统安全”要求的内容和说明。
- 4. 本标准的第7章“互联网资产、脆弱性、威胁分析”中增加了“环境和设施”类资产及其主要资产说明。
- 5. 本标准的第8章“互联网安全等级保护要求”中修改和补充了安全等级保护相关要求和内容，主要涉及8.2节、8.3节。其中，“业务及应用安全要求”部分增加了“互联网虚拟专用网服务”相关内容，主要涉及8.2.1.6节、8.3.1.6节；增加了“业务及应用系统安全要求”相关内容，主要涉及8.2.2节、8.3.2节；修改了“设备安全要求”相关内容，主要涉及8.2.3.2节、8.3.3.2节；增加了“物理环境安全要求”的相关内容，主要涉及8.2.4节、8.3.4节；删除了“移动互联网信息服务安全要求”相关内容，主要涉及原8.2.1.7节、原8.3.1.7节。

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、中国电信集团公司、中国移动通信集团公司、中国联通网络通信集团有限公司。

本标准主要起草人：杨剑锋、杨洋、田慧蓉、赵阳、刘楠、李金玉、杜之亨、张云勇。

本标准于2008年1月首次发布，本次为第一次修订。

- 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》

本标准与YD/T 1737-2009《互联网安全防护检测要求》（修订YD/T 1737-2008《互联网安全防护检测要求》）配套使用。

本标准是YD/T 1736-2008《互联网安全防护要求》的修订版本。本标准与YD/T 1736-2008的主要差异在于：

- 1. 本标准的第2章“规范性引用文件”中补充和更新了标准正文中引用的规范文件。
- 2. 本标准的第4章“缩略语”中补充和更新了标准正文中适用的缩略语。
- 3. 本标准的第5章“互联网安全防护概述”中增加了“互联网安全等级保护”相关“业务及应用系统安全”要求的内容和说明。
- 4. 本标准的第7章“互联网资产、脆弱性、威胁分析”中增加了“环境和设施”类资产及其主要资产说明。
- 5. 本标准的第8章“互联网安全等级保护要求”中修改和补充了安全等级保护相关要求和内容，主要涉及8.2节、8.3节。其中，“业务及应用安全要求”部分增加了“互联网虚拟专用网服务”相关内容，主要涉及8.2.1.6节、8.3.1.6节；增加了“业务及应用系统安全要求”相关内容，主要涉及8.2.2节、8.3.2节；修改了“设备安全要求”相关内容，主要涉及8.2.3.2节、8.3.3.2节；增加了“物理环境安全要求”的相关内容，主要涉及8.2.4节、8.3.4节；删除了“移动互联网信息服务安全要求”相关内容，主要涉及原8.2.1.7节、原8.3.1.7节。

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、中国电信集团公司、中国移动通信集团公司、中国联通网络通信集团有限公司。

本标准主要起草人：杨剑锋、杨洋、田慧蓉、赵阳、刘楠、李金玉、杜之亨、张云勇。

本标准于2008年1月首次发布，本次为第一次修订。

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》

本标准与YD/T 1737-2009《互联网安全防护检测要求》（修订YD/T 1737-2008《互联网安全防护检测要求》）配套使用。

本标准是YD/T 1736-2008《互联网安全防护要求》的修订版本。本标准与YD/T 1736-2008的主要差异在于：

1. 本标准的第2章“规范性引用文件”中补充和更新了标准正文中引用的规范文件。
2. 本标准的第4章“缩略语”中补充和更新了标准正文中适用的缩略语。
3. 本标准的第5章“互联网安全防护概述”中增加了“互联网安全等级保护”相关“业务及应用系统安全”要求的内容和说明。
4. 本标准的第7章“互联网资产、脆弱性、威胁分析”中增加了“环境和设施”类资产及其主要资产说明。
5. 本标准的第8章“互联网安全等级保护要求”中修改和补充了安全等级保护相关要求和内容，主要涉及8.2节、8.3节。其中，“业务及应用安全要求”部分增加了“互联网虚拟专用网服务”相关内容，主要涉及8.2.1.6节、8.3.1.6节；增加了“业务及应用系统安全要求”相关内容，主要涉及8.2.2节、8.3.2节；修改了“设备安全要求”相关内容，主要涉及8.2.3.2节、8.3.3.2节；增加了“物理环境安全要求”的相关内容，主要涉及8.2.4节、8.3.4节；删除了“移动互联网信息服务安全要求”相关内容，主要涉及原8.2.1.7节、原8.3.1.7节。

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、中国电信集团公司、中国移动通信集团公司、中国联通网络通信集团有限公司。

本标准主要起草人：杨剑锋、杨洋、田慧蓉、赵阳、刘楠、李金玉、杜之亨、张云勇。

本标准于2008年1月首次发布，本次为第一次修订。

- 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》

本标准与YD/T 1737-2009《互联网安全防护检测要求》（修订YD/T 1737-2008《互联网安全防护检测要求》）配套使用。

本标准是YD/T 1736-2008《互联网安全防护要求》的修订版本。本标准与YD/T 1736-2008的主要差异在于：

- 1. 本标准的第2章“规范性引用文件”中补充和更新了标准正文中引用的规范文件。
- 2. 本标准的第4章“缩略语”中补充和更新了标准正文中适用的缩略语。
- 3. 本标准的第5章“互联网安全防护概述”中增加了“互联网安全等级保护”相关“业务及应用系统安全”要求的内容和说明。
- 4. 本标准的第7章“互联网资产、脆弱性、威胁分析”中增加了“环境和设施”类资产及其主要资产说明。
- 5. 本标准的第8章“互联网安全等级保护要求”中修改和补充了安全等级保护相关要求和内容，主要涉及8.2节、8.3节。其中，“业务及应用安全要求”部分增加了“互联网虚拟专用网服务”相关内容，主要涉及8.2.1.6节、8.3.1.6节；增加了“业务及应用系统安全要求”相关内容，主要涉及8.2.2节、8.3.2节；修改了“设备安全要求”相关内容，主要涉及8.2.3.2节、8.3.3.2节；增加了“物理环境安全要求”的相关内容，主要涉及8.2.4节、8.3.4节；删除了“移动互联网信息服务安全要求”相关内容，主要涉及原8.2.1.7节、原8.3.1.7节。

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、中国电信集团公司、中国移动通信集团公司、中国联通网络通信集团有限公司。

本标准主要起草人：杨剑锋、杨洋、田慧蓉、赵阳、刘楠、李金玉、杜之亨、张云勇。

本标准于2008年1月首次发布，本次为第一次修订。

- 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》

本标准与YD/T 1737-2009《互联网安全防护检测要求》（修订YD/T 1737-2008《互联网安全防护检测要求》）配套使用。

本标准是YD/T 1736-2008《互联网安全防护要求》的修订版本。本标准与YD/T 1736-2008的主要差异在于：

- 1. 本标准的第2章“规范性引用文件”中补充和更新了标准正文中引用的规范文件。
- 2. 本标准的第4章“缩略语”中补充和更新了标准正文中适用的缩略语。
- 3. 本标准的第5章“互联网安全防护概述”中增加了“互联网安全等级保护”相关“业务及应用系统安全”要求的内容和说明。
- 4. 本标准的第7章“互联网资产、脆弱性、威胁分析”中增加了“环境和设施”类资产及其主要资产说明。
- 5. 本标准的第8章“互联网安全等级保护要求”中修改和补充了安全等级保护相关要求和内容，主要涉及8.2节、8.3节。其中，“业务及应用安全要求”部分增加了“互联网虚拟专用网服务”相关内容，主要涉及8.2.1.6节、8.3.1.6节；增加了“业务及应用系统安全要求”相关内容，主要涉及8.2.2节、8.3.2节；修改了“设备安全要求”相关内容，主要涉及8.2.3.2节、8.3.3.2节；增加了“物理环境安全要求”的相关内容，主要涉及8.2.4节、8.3.4节；删除了“移动互联网信息服务安全要求”相关内容，主要涉及原8.2.1.7节、原8.3.1.7节。

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、中国电信集团公司、中国移动通信集团公司、中国联通网络通信集团有限公司。

本标准主要起草人：杨剑锋、杨洋、田慧蓉、赵阳、刘楠、李金玉、杜之亨、张云勇。

本标准于2008年1月首次发布，本次为第一次修订。

i) 应对重要主机进行入侵行为的监测,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,并在发生严重入侵事件时提供报警;

j) 重要的通用主机应能够对重要程序的完整性进行检测,并在检测到完整性受到破坏后具有恢复的措施;

k) 通用主机防恶意代码产品应使用与网络/系统防恶意代码产品不同的恶意代码库。

8.3.4 物理环境安全要求

a) 应满足YD/T 1754-2008中第3.1级的安全要求;

b) 互联网相关业务及应用系统所处机房整体抗震能力应不低于里氏8级,相关机架及设备需进行必要的抗震加固,相关楼层承重能力不低于 1000kg/m^2 。

8.3.5 管理安全要求

应满足YD/T 1756-2008中第3.1级的安全要求。

8.4 第3.2级要求

同第3.1级要求。

8.5 第4级要求

同第3.2级要求。

8.6 第5级要求

待研究。

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要求

根据YD/T 1731-2008第5.1节要求,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 冗余系统、冗余设备及冗余链路要求

a) 业务及应用系统相关设备的处理能力应具备一定的冗余,应满足业务高峰期需要;

b) 关键设备的重要部件应采用冗余的方式提供保护;

c) 系统应具备一定的灾难备份和恢复的能力,关键设备、重要线路应采用冗余的保护方式。

9.3.2 备份数据要求

a) 应建立对业务及应用关键数据和重要信息进行备份和恢复的管理和控制机制;

b) 相关业务及应用的关键数据(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)应有必要的容灾备份;

c) 相关业务及应用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 人员和技术支持能力要求

a) 业务及应用系统的运维应有专职的管理责任人;

b) 应有系统业务管理和控制,以及设备操作、维护、管理等相关技术人员;

c) 相关管理和技术人员应通过技术培训和考核。

9.3.4 运行维护管理能力要求

a) 应具有完善运行维护管理制度，管理制度应涵盖业务管理和控制、系统运行、设备操作和维护等方面；

b) 应按照统一的运行维护要求，对业务及应用系统进行规范化的维护；

c) 应有业务及应用系统相关介质存取、验证和转储的管理制度，确保有关备份数据、信息的授权访问；

d) 应保持与其他部门、外部单位间良好的联络和协作能力。

9.3.5 灾难恢复预案要求

a) 应建立相关业务及应用系统的灾难恢复预案；

b) 应对灾难恢复预案的进行教育、培训和演练；

c) 互联网业务及应用灾难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，相关系统可用性、业务恢复时间要求见YDN 126-2009。

9.4 第3.1级要求

9.4.1 冗余系统、冗余设备及冗余链路要求

除满足9.3.1节的要求之外，还应满足：

a) 重要设备、线路应采用热备份的保护方式进行保护；

b) 系统应有必要的流量负荷分担设计；

c) 系统应具备较好的灾难备份和业务恢复的能力，提供重要服务的业务及应用系统应进行系统级备份，以保证其业务连续性。

9.4.2 备份数据要求

除满足9.3.2节的要求之外，还应满足：

a) 应建立对业务及应用全部数据、信息进行备份和恢复的管理和控制机制；

b) 系统重要的业务及应用相关数据应进行异址备份；

c) 系统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。

9.4.3 人员和技术支持能力要求

除满足9.3.3节的要求之外，还应满足：

a) 应有专职的系统业务管理和控制，以及设备操作、维护、管理等相关技术人员；

b) 相关管理和技术人员应定期组织安全技术培训和考核。

9.4.4 运行维护管理能力要求

除满足9.3.4节的要求之外，还应满足：

a) 应按介质特性对业务及应用、系统、设备相关各类备份数据进行定期的有效性验证；

b) 应制定针对业务及应用恢复、系统灾难备份的应急运行管理制度。

9.4.5 灾难恢复预案要求

除满足9.3.5节的要求之外，还应满足：

a) 应定期对灾难恢复预案的进行教育、培训和演练；

b) 应按照统一的灾难恢复预案管理制度对业务及应用相关的预案进行管理。

YD/T 1736-2009

9.5 第 3.2 级要求
同第 3.1 级要求。

9.6 第 4 级要求
同第 3.2 级要求。

9.7 第 5 级要求
待研究。

参 考 文 献

1. GB/T 18336-2000 信息技术 信息技术安全性评估准则
 2. GB/T 19716-2005 信息技术 信息安全管理实用规则
 3. GB/T 19715.2-2005 信息技术 信息安全管理指南 第 2 部分
 4. GB17859-1999 计算机信息系统安全等级划分准则
 5. 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
 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
-

中 华 人 民 共 和 国
通 信 行 业 标 准
互联网安全防护要求
YD/T 1736-2009

*

人民邮电出版社出版发行
北京市崇文区夕照寺街14号A座
邮政编码: 100061
北京新瑞铭印刷有限公司印刷
版权所有 不得翻印

*

开本: 880×1230 1/16 2010年1月第1版
印张: 1.75 2010年1月北京第1次印刷
字数: 39千字

ISBN 978 - 7 - 115 - 2014/10 - 76

定价: 15元

本书如有印装质量问题, 请与本社联系 电话: (010)67114922