YD

中华人民共和国通信行业标准

YD/T 1740-2008

增值业务网——智能网安全防护要求

Security Protection Requirements for
Value Added Service Network(Intelligent Network)

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 1741-2008《增值业务网——智能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：张大坤、张 园、李友国、王 宇、严斌峰

增值业务网——智能网安全防护要求

1 范围

本标准规定了智能网在安全等级保护、风险评估、灾难备份及恢复等方面的安全防护要求。

本标准适用于公用电信增值业务网——智能网。

2 引用标准

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文件。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 1730-2008	电信网和互联网安全风险评估实施指南
YD/T 1731-2008	电信网和互联网灾难备份及恢复实施指南
YD/T 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
YDN 048-1997	中国智能网设备业务控制点(SCP)技术规范
YDN 047-1997	中国智能网设备业务交换点(SSP)技术规范
YDN 098-1999	中国智能网设备智能外设(IP)技术规范
YDN 049-1997	中国智能网设备业务管理点(SMP)技术规范
YD/T 1234-2002	900/1800MHz TDMA数字蜂窝移动通信网业务控制点（SCP）设备技术要求（CAMEL2）
YD/T 1425-2005	900/1800MHz TDMA数字蜂窝移动通信网业务控制点（SCP）设备技术要求（CAMEL3）
YD/T 1209-2002	900/1800MHz TDMA数字蜂窝移动通信网业务交换点（SSP）设备技术要求（CAMEL2）
YD/T 1424.1-2005	900/1800MHz TDMA数字蜂窝移动通信网业务交换点（SSP）设备技术要求（CAMEL3）第1部分：电路域（CS）
YD/T 1424.2-2005	900/1800MHz TDMA数字蜂窝移动通信网业务换点（SSP）设备技术要求（CAMEL3）第2部分：分组域（PS）
YD/T 1427-2005	900/1800MHz TDMA数字蜂窝移动通信网智能外设（IP）设备技术要求（CAMEL3）
YD/T 1426-2005	900/1800MHz TDMA数字蜂窝移动通信网业务管理点（SMP）设备技术要求（CAMEL3）
YD/T 1232-2002	800MHz CDMA数字蜂窝移动通信网无线智能网（WIN）阶段1：业务控制点（SCP）设备技术要求

YD/T 1333-2004	800MHz CDMA数字蜂窝移动通信网无线智能网（WIN）阶段2：业务控制点（SCP）设备技术要求
YD/T 1223-2002	800MHz CDMA数字蜂窝移动通信网无线智能网（WIN）阶段1：业务交换点（SSP）设备技术要求
YD/T 1334-2004	800MHz CDMA数字蜂窝移动通信网无线智能网（WIN）阶段2：智能外设（IP）设备技术要求
YD/T 1332-2004	800MHz CDMA数字蜂窝移动通信网无线智能网（WIN）阶段2：业务管理点（SMP）设备技术要求

3 术语和定义

下列术语和定义适用于本标准。

3.1

智能网安全等级 Security Classification of Transport Network

智能网安全重要程度的表征。重要程度可从智能网受到破坏后，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。

3.2

智能网安全等级保护 Classified Security Protection of Intelligent Network

对智能网分等级实施安全保护。

3.3

组织 Organization

组织是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。

3.4

智能网安全风险 Security Risk of Intelligent Network

人为或自然的威胁可能利用智能网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。

3.5

智能网安全风险评估 Security Risk Assessment of Intelligent Network

指运用科学的方法和手段，系统地分析智能网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，进一步提出有针对性的防护对策和安全措施，防范和化解智能网安全风险，将风险控制在可接受的水平，为最大限度地保障智能网的安全提供科学依据。

3.6

智能网资产 Asset of Intelligent Network

智能网中具有价值的资源，是安全防护保护的对象。智能网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。如基于某个智能网系统的预付费业务，SCP设备，智能网机房管理规定等。

3.7

智能网资产价值 Asset Value of Intelligent Network

智能网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。

3.8

智能网威胁 Threat of Intelligent Network

可能导致对智能网产生危害的不希望事件的潜在起因。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。常见的有设备节点失效、火灾、水灾等。

3.9

智能网脆弱性 Vulnerability of Intelligent Network

脆弱性是智能网中存在的弱点、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及资产的安全。

3.10

智能网灾难 Disaster of Intelligent Network

由于各种原因，造成智能网故障或瘫痪，使智能网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。

3.11

智能网灾难备份 Backup for Disaster Recovery of Intelligent Network

为了智能网灾难恢复而对相关网络要素进行备份的过程。

3.12

智能网灾难恢复 Disaster Recovery of Intelligent Network

为了将智能网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。

CDMA	Code Division Multiple Access	码分多址
GSM	Global System for Mobile Communication	全球移动通信系统
IP	Intelligent Peripheral	智能外设
SCP	Service Control Point	业务控制点
SDP	Service Data Point	业务数据点
SMP	Service Management Point	业务管理点
SSP	Service Switch Point	业务交换点
VC	Voucher Center	充值中心
VPN	Virtual Private Network	虚拟专用网

5 智能网系统安全防护概述

5.1 智能网安全防护范围

智能网是指在原有电信交换网络基础上，为快速提供新的电信业务而叠加的网络。智能网包括业务控制点（SCP）设备、业务交换点（SSP）设备、业务管理点（SMP）设备、智能外设（IP）设备、业务数据点（SDP）设备和充值中心（VC），其中SCP实现业务的集中控制，SSP实现业务触发，SMP实现业务管理，IP实现自动语音播放与采集，SDP实现智能业务数据集中放置，VC是智能业务的充值中心。

本标准中的“智能网系统”指基于以上设备及设备之间的网络组成的智能网系统，根据所依附的网络可以分为固定智能网、GSM智能网和CDMA智能网，根据覆盖范围可以分为本地智能网、全省智能网和全国智能网。

5.2 智能网安全防护内容

根据电信网和互联网安全防护体系的要求，将智能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3个部分。

智能网安全等级保护主要包括定级对象和安全等级确定、业务安全、网络安全、设备安全、物理环境安全、管理安全等；

安全风险评估主要包括资产识别、脆弱性识别、威胁识别、已有安全措施的确认、安全风险分析、安全风险评估文件处理等，本标准仅对智能网进行资产分析、脆弱性分析和威胁分析，在智能网安全风险评估过程中确定各个资产、脆弱性、威胁的具体值。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》；

智能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 智能网定级对象和安全等级确定

根据智能网业务对公众利益的影响程度、所提供服务的重要性及服务用户数的多少几个关键因素，我国智能网可以分为全国智能网、省内智能网和本地智能网，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》中确定网络安全等级的方法，根据网络的具体情况，对整个智能网系统进行定级，权重α、β、γ可根据具体网络情况进行调节。

7 智能网资产、脆弱性、威胁风险分析

7.1 资产分析

智能网安全风险评估的资产至少应包括设备硬件、设备软件、重要数据、提供的服务、文档、人员等，见表1。

表1 资产列表

分 类	示 例
设备硬件	智能网包括 SCP、SDP、SSP、SMP、IP、VC 等设备； 物理环境设备：包括机房、电力供应系统、电磁防护系统、防火、防水和防潮系统、防静电系统、防雷击系统、温湿度控制系统等； 网络：设备之间的信令链路等
设备软件	系统软件：操作系统、各种数据库软件等； 协议软件和控制软件
重要数据	保存在设备上的各种重要数据，包括用户数据、计费数据、网络配置数据、管理员操作维护记录等
服务/业务	智能网提供的各种业务：预付费、VPN、被叫付费电话等
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	掌握重要技术的人员，如网络维护人员、设备维护人员、网络或业务的研发人员等
其他	网络拓扑设计等

7.2 脆弱性分析

智能网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，部分脆弱性识别内容见表2。

表2 脆弱性分析

类 型	对 象	存在的脆弱性
技术脆弱性	业务/应用	系统本身设计缺陷或软件Bug； 网络和设备的处理能力不够而导致在突发话务量高时业务提供不连续，业务数据的保密性不够，重要数据未及时进行本地和异地备份； SSP处理能力不够导致智能网无法正常提供业务； 网管、操作维护存在漏洞； 业务软件自身存在的安全漏洞； SCP单点设置
	网络	网络拓扑设计不合理，网络节点设备、路由配置不合理，通信安全保护不充分，外部和内部的访问缺少控制等
	设备（含操作系统和数据库）	账号和口令保护不够，鉴权和访问控制机制不完善，重要部件未配置主备用保护，系统配置不合理，备份和恢复机制不健全，设备超过使用年限或核心部件老化，设备发生故障后未及时告警，软件版本管理不规范
	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、机房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

脆弱性大小由网络和业务运营商自行赋值。

7.3 威胁分析

智能网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。部分威胁见表3。

表3 威胁来源列表

来 源		威胁描述
设备威胁		设备自身的软件、硬件故障； 节假日或其他原因的高话务量冲击； 滥用权限对操作维护数据的修改
环境威胁	物理环境	断电、静电、灰尘、潮湿、温度、强电磁干扰等，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、闪电

表3（续）

来 源		威胁描述
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； 采用自主外部人员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
	无恶意人员	内部人员由于缺乏责任心或者无作为，应该执行而没有执行相应的操作，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

8 智能网网安全等级保护要求

8.1 第1级

不作要求。

8.2 第2级

8.2.1 智能网业务安全要求

a）管理员密码等数据应该进行加密处理，而不应在文件或数据库中明文显示；

b）计费信息应正确、不丢失、不重复，计费信息不能被修改，原始话单不能被增加；

c）卡号、密码的鉴权采用一定的安全机制，如限制尝试次数。

8.2.2 智能网网络安全要求

智能网网络中（如SCP和SMP、SMP与账务系统之间）应采用专网方式。

8.2.3 智能网设备安全要求

8.2.3.1 概述

智能网包括业务控制点（SCP）设备、业务交换点（SSP）设备、业务管理点（SMP）设备、智能外设（IP）设备、业务数据点（SDP）设备和充值中心（VC）设备，可以服务于固定网、GSM网和CDMA网络。

设备安全应满足相关设备技术规范、设备安全要求、设备入网管理相关要求。

8.2.3.2 固定智能网

a）SCP设备应满足YDN 048-1997的要求；

b）SSP设备应满足YDN 047-1997的要求；

c）IP设备应满足YDN 098-1999的要求；

d）SMP设备应满足YDN 049-1997的要求。

8.2.3.3 GSM智能网

a）SCP设备应满足YD/T 1234-2002和YD/T 1425-2005的要求；

b）SSP设备应满足YD/T 1209-2002、YD/T 1424.1-2005和YD/T 1424.2-2005的要求；

c）IP设备应满足YD/T 1427-2005的要求；

d）SMP设备应满足YD/T 1426-2005的要求。

8.2.3.4 CDMA 智能网

a）SCP设备应满足YD/T 1232-2002和YD/T 1333-2004的要求；

b）SSP设备应满足YD/T 1223-2002和YD/T 1331-2004的要求；

c）IP设备应满足YD/T 1334-2004的要求；

d）SMP设备应满足YD/T 1332-2004的要求。

8.2.4 智能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》中第2级的安全要求。

8.2.5 智能网管理安全要求

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

8.3 第 3.1 级

8.3.1 智能网业务安全要求

在满足第2级的基础上，还应满足以下要求：

a）特定智能网业务的使用和开展要具有一定的安全机制，如用户名/密码的加密传输，卡号生成、传输、管理的安全机制等。

b）应保证在运行的智能网系统上引入新业务、升级业务或系统时不会引起智能网所提供业务的中断或系统瘫痪。

8.3.2 智能网网络安全要求

在满足第2级的基础上，还应满足以下要求：

a）智能网的网络配置（如节点和链路的处理能力或负荷等）应合理，不应因网络配置不合理而导致网络全部或者局部瘫痪；

b）网络拓扑（如信令链路、话路）设计中，应当充分考虑连接的冗余设置，不应存在因单点故障而影响其他节点间数据传送的节点。

8.3.3 智能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》中第3.1级的安全要求。

8.3.4 智能网管理安全要求

应满足YD/T 1756-2008《电信网和互联网管理安全等级保护要求》中第3.1级的安全要求。

8.4 第 3.2 级

8.4.1 智能网业务安全要求

在满足第3.1级的基础上，还应满足以下要求：

重要业务数据及计费数据应进行备份（包括不同物理位置、不同存储格式、不同存储介质等），以防止各种原因导致的系统崩溃。

8.4.2 智能网网络安全要求

在满足第3.1级的基础上，还应满足以下要求：

重要设备应实现异地备份，互为备份的设备应在两个不同的机房。

8.4.3 智能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》中第3.2级的安全要求。

8.4.4 智能网管理安全要求

应满足YD/T 1756-2008《电信网和互联网管理安全等级保护要求》中第3.2级的安全要求。

8.5 第4级

同第3.2级要求。

8.6 第5级

待补充。

9 智能网灾难备份及恢复要求

9.1 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

不作要求。

9.3 第2级

9.3.1 冗余系统、设备及链路要求

a）智能网应具备一定的抗灾难以及灾难恢复能力，以保证在各个方面出现故障时都有备用系统提供服务，包括：重要设备部件的成对配置，如网卡、信令板卡、业务板卡等。

b）智能网网络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 冗余路由要求

a）应有流量负荷分担设计；

b）智能网的业务中断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。

9.3.3 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 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）应有针对灾难备份及恢复的介质存取、验证和转储的管理制度，应确保备份数据的授权访问；

9.3.5 灾难恢复预案要求

应有完整的灾难恢复预案。

9.4 第3.1级

9.4.1 冗余系统、设备及链路要求

在满足第2级的基础上，还应满足以下要求。

智能网应具备一定的抗灾难以及灾难恢复能力，以保证在各个方面出现故障时都有备用系统提供服务，包括：软件系统的冗余，如业务软件的备份等。

9.4.2 备份数据要求

在满足第2级的基础上，还应满足以下要求。

智能网关键数据应有本地数据备份，包括：

- 业务数据和用户数据，如 VPN 业务中的长号码、短号码、组信息、费率信息和用户属性等；
- 网络配置数据，如路由数据等；
- 告警数据，如告警历史信息等；
- 加密密钥数据。

9.4.3 人员和技术支持能力要求

在满足第 2 级的基础上，还应满足以下要求：

a）应有负责灾难备份及恢复的设备管理人员；

b）应有负责灾难备份及恢复的网络管理人员；

c）应有负责灾难备份及恢复的技术支持人员；

d）应对负责灾难备份及恢复的人员定期进行关于灾难备份及恢复的技术培训。

9.4.4 运行维护管理能力要求

在满足第 2 级的基础上，还应满足以下要求：

a）应对灾难备份及恢复相关数据进行定期的有效性验证；

b）应有针对灾难备份及恢复的设备和网络运行管理制度；

c）应具有与外部组织保持良好的联络和协作的能力。

9.4.5 灾难恢复预案要求

在满足第 2 级的基础上，还应满足以下要求：

a）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；

b）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。

9.5 第 3.2 级

9.5.1 冗余系统、设备及链路要求

在满足第3.1级的基础上，还应满足以下要求：

智能网应具备一定的抗灾难以及灾难恢复能力，以保证在各个方面出现故障时都有备用系统提供服务，包括：设备的异地备份，如 SCP、VC 等设备。

9.5.2 冗余路由要求

在满足第3.1级的基础上，还应满足以下要求：

对于重要地区，智能网设备之间的路由应支持冗余方式，包括SCP和SSP之间、SCP和IP之间、SCP和SDP之间及SSP和IP之间的路由等。

9.5.3 备份数据要求

在满足第3.1级的基础上，还应满足以下要求：

智能网重要数据（如业务数据、网络配置数据、告警数据、加密密钥等）等应有异地容灾数据备份。

9.5.4 运行维护管理能力要求

在满足第3.1级的基础上，还应满足以下要求：

应有针对灾难备份及恢复的数据异地实时容灾备份管理制度。

9.5.5 灾难恢复预案要求

在满足第3.1级的基础上，还应满足以下要求：

应有完善的灾难恢复预案管理制度。

9.6 第4级

同第3.2级要求。

9.7 第5级

待补充。