

YDN

通 信 技 术 规 定

YDN 126-2005

增值电信业务 网络信息安全保障基本要求

Baseline requirements for network and information security of
value-added telecommunication services

2005-04-28 发布

2005-10-01 实施

中华人民共和国信息产业部 发布

目 次

前 言	II
引 言	III
1 范围	1
2 规范性引用文件	1
3 定义和缩略语	1
3.1 定义	1
3.2 缩略语	2
4 增值电信业务	2
5 增值电信业务网络所面临的安全风险	3
5.1 综述	3
5.2 增值电信业务网络安全保护对象	3
5.3 增值电信业务网络所面临的安全威胁	3
6 安全保障措施要求	4
6.1 综述	4
6.2 信息资源安全保障措施	4
6.3 硬件设备和环境安全保障措施	5
6.4 网络安全保障措施	6
6.5 平台系统软件安全保障措施	7
6.6 业务应用系统安全保障措施	8
附录 A (规范性附录) 因特网接入服务 (ISP) 业务安全保障要求	9
附录 B (规范性附录) 信息服务业务安全保障要求	10
附录 C (规范性附录) 国内多方通信服务安全保障要求	11
附录 D (规范性附录) 在线数据处理与交易处理业务安全保障要求	12
附录 E (规范性附录) 存储转发类业务安全保障要求	13
附录 F (规范性附录) IDC 业务安全保障要求	14
附录 G (规范性附录) 国内因特网虚拟专用网业务安全保障要求	15
附录 H (规范性附录) 呼叫中心业务安全保障要求	16
附录 I (资料性附录) 增值电信业务分类	17

前 言

本标准是依据《电信运营重大事故报告规定（试行）》、《电信服务标准》、《中华人民共和国电信条例》附则《增值电信业务分类》、《互联网信息服务管理办法》制定的，是为保证增值电信业务网络信息安全而制定的基本要求。

本标准的附录A、附录B、附录C、附录D、附录E、附录F、附录G、附录H为规范性附录。

本标准的附录I为资料性附录。

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

本标准主要起草人：谢 玮 傅景广 孙明俊 葛 坚

引 言

本标准的技术内容包括三部分：第4章增值电信业务定义和分类描述；第5章增值电信业务安全风险分析，第6章安全保障措施要求。

本标准第5、6章内容是对增值电信业务提供商的具体安全要求，其中，第5章要求增值电信业务提供商在确定自身业务网络安全保护的对象，并明确其所面临的安全威胁的基础上，制定安全保障策略和措施；而第6章则详细规定了安全保障措施要求的具体内容。

标准的附录A到附录H是对第6章中业务层安全技术要求不同种类增值业务的细化。

增值电信业务网络信息安全保障基本要求

1 范围

本标准规定了增值电信业务网络信息安全保障措施基本要求，包括信息资源安全要求、硬件设备和环境安全要求、网络安全要求、平台系统软件安全要求、业务应用系统安全要求等内容。

本标准适用于我国增值电信业务网络信息安全保障体系的建设，是增值电信业务提供商建立自身网络信息安全保障框架、增值电信业务监管机构检查经营者安全保障措施实施情况的重要依据。本标准中的网络信息安全保障措施是基本要求，各企业可能需要根据本企业业务特点制定不包括在本标准内的其它安全保障措施。

本标准中的安全技术保障措施要求是指各种设备、系统所要具备的安全功能，应通过设备和系统的功能说明书体现。

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 1132-2001

防火墙设备技术要求

YD/T 1311-2004

防范互联网垃圾电子邮件技术要求

3 定义和缩略语

3.1 定义

本标准采用下列定义。

- 增值电信业务（Added-Value Telecommunication Service）：
凭借公用电信网的资源和其它通信设备而开发的附加通信业务，其实现的价值使原有网络的经济效益或功能价值增高。
- 增值电信业务提供商（Added-Value Telecommunication Service Provider）：
提供增值电信业务内容或应用平台的企业，包括增值电信业务内容提供商和增值电信业务平台提供商。
- 增值电信业务内容提供商（Content Provider of Added-Value Telecommunication Service）：
提供增值电信业务内容的企业。
- 增值电信业务平台提供商（Platform Provider of Added-Value Telecommunication Service）：
提供增值电信业务应用平台的电信企业。
- 基础电信业务运营商（Baseline Telecommunication Service Provider）：
为增值电信业务提供基础网络传输服务的电信企业。
- 平台系统软件（Platform System Software）：
为业务应用程序提供平台服务的软件，如操作系统、中间件等。
- 业务应用系统（Service Application System）：

指建立在平台系统之上, 进行业务数据处理和提供业务服务的软件系统。

3.2 缩略语

本标准采用下列缩略语:

AAA	Authentication, Authorization and Accounting	认证、授权和计费
B2C	Business to Customer	商业机构对消费者的电子商务
CP	Content Provider	内容提供商
DDN	Digital Data Network	数字数据网
ICP	Internet Content Provider	因特网内容提供商
IDC	Internet Data Center	因特网数据中心业务
IDS	Intrusion Detection System	入侵检测系统
IP	Internet Protocol	因特网协议
IP VPN	IP Virtual Private Network网	因特网虚拟专用
IPSec	IP Security	IP安全
ISP	Internet Service Provider	因特网接入服务
PKI	Public Key Infrastructure	公钥基础设施
TCP	Transmission Control Protocol	传输控制协议
VOD	Video On Demand	视频点播

4 增值电信业务

增值电信业务是凭借公用电信网的资源和其它通信设备而开发的附加通信业务, 其实现的价值使原有网路的经济效益或功能价值增高。

增值电信业务分为两大类, 共8小类:

—— 第一类增值电信业务

- 在线数据处理与交易处理业务;
- 国内多方通信服务业务;
- 国内因特网虚拟专用网 (IP-VPN) 业务;
- 因特网数据中心 (IDC) 业务。

—— 第二类增值电信业务

- 存储转发类业务 (含语音信箱、X.400 电子邮件业务、传真存储转发业务、语音邮件和增值传真存储转发业务等);
- 呼叫中心业务;
- 因特网接入服务 (ISP) 业务;
- 信息服务业务[含电话信息服务 (声讯服务)、因特网信息服务、通信短消息服务、和电子邮件]。
- 各类业务的详细说明参见本标准附录 I。

5 增值电信业务网络所面临的安全风险

5.1 综述

不同的增值电信业务需要进行安全保护的对象以及面临的具体安全威胁会有所不同，增值电信业务提供商应当能够根据自己的承载网络和业务类型具体分析。

5.2 增值电信业务网络安全保护对象

增值电信业务网络中需要进行安全保护的对象至少包括：

- 物理设备；
- 通信网络；
- 平台系统软件；
- 业务应用系统。

下面逐一加以描述。

—— 物理设备，包括：

- 网络通信设备。增值电信业务网络通常承载在基础电信网络运营商提供的传输网络上，对于这部分网络资源的安全保护不属于本标准范围，因此这里的设备仅指增值电信业务网络自身所需要维护的设备，例如本地交换机、防火墙、路由器、各种应用服务器、数据库服务器等。
- 用户终端设备。包括用户使用增值电信业务的终端主机等。对于这部分网络资源的安全保护不属于本标准范围。
- 其他硬件设备，比如操作维护终端、打印机、存储设备、电源等。

—— 通信网络，包括：

- 通信网络操作信息，保证网络正常工作的数据，例如通信网络配置数据、路由选择表、用户数据表等。
- 无形的网络资源，比如带宽和速率。

—— 平台系统软件，包括：

- 子系统操作信息，保证子系统正常工作的数据，例如操作系统配置信息、数据库系统配置信息等。
- 操作系统软件和数据库系统软件。

—— 业务应用系统，包括：

- 业务应用系统软件。
- 业务运营信息（例如业务运营日志、计费信息等）。
- 向用户提供的各种信息（例如发布的新闻信息等）。
- 用户个人注册信息。
- 用户虚拟存储空间中信息，例如电子邮箱中电子邮件等。

5.3 增值电信业务网络所面临的安全威胁

根据以上确定的安全保护对象，增值电信业务网络可能面临的安全威胁分为以下几类：

1. 物理设备安全威胁：指增值电信业务网络物理设备可能遭到的物理损害，例如自然灾害、由于电力系统问题而造成的物理设备失效等。
2. 通信网络安全威胁：指增值电信业务网络实体可能面临的攻击，包括黑客对网络设备的攻击、对网络资源（比如带宽、存储空间等）的非法占用、以及对维持网络正常运行的数据信息的攻击（包括非法访问、修改、删除等）。

3. 平台系统软件安全威胁：指针对操作系统和系统数据库的攻击，例如利用操作系统本身漏洞对其进行的 DOS 攻击、专门感染操作系统的病毒及恶意代码、对于系统数据库数据的恶意访问和非法操作等等。
4. 业务应用安全威胁，包括：
 - 黑客的攻击：实际上黑客的攻击手段种类繁多，比如利用系统后门对提供业务的主机进行破坏，造成业务中断，或者对业务网络或服务器进行拒绝服务攻击，消耗业务资源，使无法正常向用户提供信息服务。目前通常采取设置防火墙的方法阻止黑客的攻击。
 - 病毒及恶意代码的干扰，防病毒软件可以在一定程度上防止或减轻病毒和恶意代码造成的损害。
 - 业务运营商内部员工的非法行为（比如非法进入机密数据库，删除修改数据，泄漏重要安全信息等）以及操作员在运营维护中出现的错误或失误。这些行为实际上都是可以通过完善的安全管理制度尽量避免。在发生问题时，应能通过及时的应急措施和业务恢复措施尽量减少问题的影响。
 - 对业务网络中传输和存储的数据信息（包括私人信息、保密信息、敏感的金融信息等等）的盗窃行为，对于数据盗窃的防护措施主要是加密技术、严格的访问控制机制、操作的可审计性等。
 - 非法信息传播：导致这种威胁出现的手段很多，例如黑客篡改网页导致出现非法信息传播、利用增值业务应用系统中的 BBS 平台进行非法信息传播等等。

6 安全保障措施要求

6.1 综述

增值电信业务提供商应从以下几个方面制定并实施自身业务网络的安全保障措施：

- 信息资源安全保障措施；
- 硬件设备和环境安全保障措施；
- 网络安全保障措施；
- 平台系统软件安全保障措施；
- 业务应用系统安全保障措施。

下面章节将分别加以论述。

6.2 信息资源安全保障措施

6.2.1 信息类资产安全

信息类资产是指数据文件、系统文件、操作或执行程序、用户信息、业务信息等非实物资产。保证信息资产安全应做到：

1. 为重要信息类资产建立资产清单。所有资产清单应具有统一格式，如文件所有者、卷系列号、文件名及其描述、作业或项目编号、建立日期及保存期限、安全保护等级等等。
2. 对所有信息类资产根据其不同属性进行分类，并采取有效的措施，比如建立索引，方便查找。
3. 根据信息的保密性和重要性确定安全等级。对于不同安全等级的信息资产应制定不同的管理规范和管理制度。各企业应根据自身的具体情况界定信息的安全级别。增值电信业务提供商可以将本业务网络内的信息分为两大类：一般信息（不会对业务运行产生重要影响的信息，例如 Web 服务器上供用户浏览的信息、用户间传送的信息等）、重要信息（影响业务运行的信息，例如系统

配置信息、业务网络配置信息、用户业务日志、用户账户信息等等)。其中重要信息可以再细分级别:非涉密级信息、秘密级信息。具体的划分原则各企业应根据实际情况而定^①。

6.2.2 信息发布安全

信息发布是指将业务信息通过网络提供给用户检索或浏览,例如提供Web页面、发送订阅短信息等等。保证信息发布安全应做到:

1. 增值电信业务内容提供商的数据输出控制应有专人负责,明确负责人的职责。输出文件在发到用户之前,应由数据处理部门进行审核。
2. 对于用户利用增值电信业务提供商的网络资源发布的信息,增值电信业务提供商应能够建立相应有效的有害信息检查机制和投诉受理制度。
3. 增值电信业务内容提供商对外发布的公共信息(指文字信息)应使用专门的程序对关键字进行过滤。通过过滤的信息应有专人进行二次过滤,经过滤剔除的信息也应有专人进行复查,防止误判。
4. 提供通信短消息服务的增值电信业务内容提供商(包括CP、ISP)和增值电信业务平台提供商(这里指移动短消息平台提供商),应设立专门人员和网络资源接受并及时处理用户对于垃圾短信的投诉。
5. 对于向公众发布的声讯信息、多媒体信息,增值电信业务内容提供商应采用人工方式进行有害信息的检查。

6.2.3 信息交换安全

信息交换包括企业内部部门、人员之间的信息交换和企业与外部之间的信息交换,例如电子邮件、用户注册、发送订单、信息采集过程中的文件传递等。信息交换安全是指防止在信息交换过程中信息丢失、被修改或者盗用。保证信息交换安全应做到:

1. 对于信息交换过程进行监管,可以采取人工进行事前事后的检查和复查、或自动技术手段进行监督。
2. 对于交换的信息文件要采取一定的手段保证其保密性和完整性(例如通过数据网络进行交换的信息应采用必要的技术安全措施等),防止在交换的过程中信息丢失,被更改等情况的出现。

6.3 硬件设备和环境安全保障措施

6.3.1 设备操作安全

设备操作安全是规范设备操作流程,避免人为误操作或者未经授权的操作所导致的安全问题,并使设备操作行为具有可审计性。

- 设备和系统应有专门的人员进行操作。
- 增值电信业务提供商应制定完备的系统维护制度:
 1. 对系统进行维护时,应采取数据保护措施,如数据转储、卸下磁盘磁带等。
 2. 对系统进行预防维修或故障维修时,应记录故障原因、维修对象、维修内容和维修前后状况等信息。
 3. 应建立完整的维护记录档案。

^① IDC业务的信息分类原则待定。

——增值电信业务提供商应制定系统运行记录编写制度。系统运行记录包括系统名称、姓名、操作时间、处理业务名称、故障记录及处理情况等。重要的日志应由安全负责人签名，规定保存期限。存放重要信息的计算机（参见6.2.1节）日志应记录如下内容：

1. 每次成功的使用：记录节点名、用户名、终端名、上下机时间、操作的数据或程序名、操作的类型、修改前后的数据值。
2. 用户每次越权存取的操作：记录节点名、用户名、终端名、时间、欲越权存取的数据及操作类型、存取失败的原因。
3. 每次不成功的用户身份：记录节点名、用户名、终端名、时间。

——增值电信业务提供商的托管设备应与托管方签订相关的操作安全方面的协议。

6.3.2 物理设备和环境安全

本节的要求暂不包括增值电信业务提供商的设备被托管的情况，托管设备和环境的安全待定。

保证系统平台的硬件设备和环境安全应做到以下几点：

1. 为物理设备建立资产清单，并根据其重要性划分安全等级，例如，一般设备（一般的操作终端、打印机等，其故障不会对整个业务网络产生重大影响的设备）、重要设备（比如计费服务器、存放重要信息的数据库、基础网络设施等等）。
2. 为重要的设备选择一个安全的位置，主要包括：
 - a) 在放置该设备的房间的入口等处，应使用监控装置（如摄像头或照相机）；
 - b) 进入该地点应有一定的检查机制；
 - c) 对于某些非常重要的业务网络设施（例如接线柜等），除经过授权的必须访问以外，应严格禁止对其的访问。
3. 保证设备的电力供应，任何电力供应系统均不应超载，同时应设置备用电源以保证断电时的电力供应。
4. 应充分考虑在自然灾害发生时，设备的冗余设计能够最大限度保证业务连续性。

6.4 网络安全保障措施

增值电信业务网络的传输安全应当由提供网络承载的基础电信业务运营商来负责，因此这方面的安全要求超出了本标准的范围。本节仅规定增值电信业务网络自身管辖的网络安全（例如本地局域网网络安全）。

1. 增值电信业务网络中应采用有效手段（如防火墙或者其他类型防网络攻击的软/硬件、入侵检测系统（IDS）^②、蜜罐技术^③等）来保证本地网络安全，抵御来自公共网络的入侵。防火墙或者其他类型防网络攻击的软/硬件以及入侵检测系统（IDS）的功能要求参见 YD/T 1132-2001《防火墙设备技术要求》。
2. 业务网络应做到对外（不只是指外部网络，甚至包括内部局域网中的某些其它设备或终端）屏蔽重要设备（例如计费服务器、存放重要信息的数据库、基础网络设施等）的地址。
3. 服务器应关闭与本身服务不相关的端口。

② 入侵检测作为一种积极主动的安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。它可以弥补防火墙的不足，为网络安全提供实时的人侵检测及采取相应的防护手段，如记录证据用于跟踪、恢复、断开网络连接等。

③ 一种在网络设计中，引诱攻击者对其进行攻击，从而收集攻击者信息的类似陷阱的安全技术。

4. 企业内部存储重要信息（参见 6.2.1 节）的网络 / 计算机应该与公共网络隔离（可以采用私有地址）。

6.5 平台系统软件安全保障措施

由于大多数增值电信业务应用系统都是基于计算机操作系统和数据库系统之上开发的，因此本节对平台系统层面软件的安全保障措施的要求适用于所有种类的增值电信业务，其中如果有对于某种业务的特殊要求，将有明确标注。

增值电信业务网络平台系统软件的安全根据需要保护的对象可以分为以下两类：

- 操作系统安全；
- 系统数据库安全。

下面分别描述具体的措施要求。

6.5.1 操作系统安全

增值电信业务平台系统的操作系统软件应具备的安全保护功能包括：

- 系统应能够提供各种安全防护能力，例如文件访问控制、用户访问权限级别控制、IP 地址控制、端口安全管理等；
- 系统应具备完善的操作日志记录功能；
- 系统应提供重要数据（参见 6.2.1 节）备份功能，比如提供自动备份软件等；
- 系统和软件在任务正常或非正常结束以后，应该清除分配给该任务的全部临时工作区域。
- 除了以上操作系统的安全功能外，为保证平台系统的安全，增值电信业务提供商还应能够做到：有专人负责进行软件升级，查看最新的系统安全公告，及时为系统打补丁（系统补丁公布之后，应在 4 周之内完成涉及安全问题的补丁的测试以及测试通过后的系统升级工作，在补丁进行测试和升级工作进行期间，必须采取必要的应急安全防护措施，避免相应的安全问题发生。）等工作。
- 应定期（至少 1 个月）进行一次系统漏洞扫描。
- 如果系统采用口令识别技术，则系统的口令不得少于 6 位，口令应具有一定的复杂性，定期（至少每 3 个月）变更 1 次，核心系统的口令不得少于 8 位，至少每个月应变更 1 次。鼓励采用其他安全性更强的识别技术，如数字证书等。
- 系统应安装防病毒软件 / 硬件，根据病毒预告应随时下载安装最新的病毒库。应设专人负责查看最新的病毒公告。出现破坏力强的病毒要及时向公司相关部门通告。
- 使用下载的外部文件前应进行病毒等恶意代码及破坏性程序的检查，确认无问题后才能使用。
- 应至少每 1 个月 1 次对平台系统的配置信息进行备份。

6.5.2 数据库系统安全

对增值电信业务网络数据库系统的安全保护措施包括：

- 数据库本身应具备严格的存取访问控制机制，应能够采取层次、分区、表格等各种授权方式，控制用户对数据库的存取权限。
- 操作员对数据库访问应设置口令保护，口令长度不得小于 6 位，口令应具有一定的复杂性，至少每 2 个月应变更一次，应能够对口令表进行加密，以保护数据安全。
- 数据库对输入数据应能够进行逻辑检验，以保证数据库更新时数据的准确性。
- 对于存放重要信息的数据库（参见 6.2.1 节），应采用数据加密技术以及数据库加密技术来保护数据库的安全。
- 数据库数据应定期（至少每 1 个月 1 次）进行备份。
- 数据库软件应具备操作日志记录功能。
- 数据库软件应具备从各种人为故障、软件故障和硬件故障中进行恢复的能力。

- 数据库的所有操作均应有操作记录，以备安全审计使用。

6.6 业务应用系统安全保障措施

6.6.1 通用性要求

1. 对特定的业务终端设备，如可对重要数据（参见 6.2.1 节）进行存取的、有控制台功能的终端等，应限定操作人员。限定操作人员的方法有：口令、识别码等资格认定或设置终端设备的钥匙等。
2. 业务应用系统应能够对操作员的访问权限进行分级，并且对操作员的访问进行认证 & 授权，每个操作员应设置口令，口令长度不得小于 6 位，至少每 2 个月应变更 1 次。
3. 业务应用系统应能够对操作员的所有操作都进行详细的日志记录。
4. 业务应用系统应能够在操作员进行非法操作时自动发出告警，告警应根据行为的严重程度进行分级。告警方式应根据级别不同而不同。
5. 应至少 1 个月 1 次对重要业务数据进行备份。重要数据（参见 6.2.1 节）的备份应至少保留 3 个月。
6. 重要的业务系统在建立时就应该考虑设备备份。如主机备份、系统备份等。
7. 备份系统应定期（至少 1 年 1 次）进行实际运行，以检验备份系统的可靠性。

6.6.2 不同业务类型区别要求

业务应用层面的安全保障措施还应根据增值电信业务种类，包括承载网络性质（电路交换 / 分组交换网）和业务属性（普通业务 / 对安全敏感的业务）的不同有各自的区别要求。对应于每种类型增值电信业务业务应用层面的特殊性安全保障措施要求，参见本标准附录 A 到附录 H。

附录A

(规范性附录)

因特网接入服务 (ISP) 业务安全保障要求

ISP业务为各类用户提供接入因特网的服务。其最主要的安全指标就是保证所提供业务的可用性和业务可恢复性。ISP的业务网络应保证以下安全要求:

1. 保证所提供的因特网接入服务业务的可用性、可恢复性达到一定的性能指标。
 - 可用性: 排除外力因素 (非本企业可控制的因素), 其业务可用性应 $\geq 99.99\%$, 业务可用性是指用户能够使用本业务的时间占业务全部工作时间的百分数。95%以上的授权用户能够成功使用业务提供商所提供的因特网接入业务, 则该业务可用。
 - 可恢复性: 应做到在业务中断后, 在可接受的时间范围内 (业务恢复时间间隔平均 $\leq 4\text{h}$, 最长为 $8\text{h}^{\text{④}}$) 恢复业务, 且在最大程度上保护业务数据的完整性。
2. 应提供有效可靠的接入认证、授权和计费机制。
3. 应能够记录业务日志 (至少包括上网用户的上网时间、用户账号、因特网地址或者域名、主叫电话号码等信息), 并且应保留一定期限 (至少60天)^⑤。

④ 参照《电信服务标准》中“因特网服务质量指标”项中有关通信设备障碍修复时限的数值。如果该法规修订, 则本标准应作相应改动。

⑤ 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。

附录B

(规范性附录)

信息服务业务安全保障要求

信息服务业务含电话信息服务(声讯服务)、因特网信息服务和电子邮件、通信短消息服务。由于该类业务可以向公众提供信息服务,具有媒体性质,因此其业务运营、信息内容、用户接入等方面的安全要求则相对较为严格。

B.1 业务应用系统信息内容存储、传输安全技术要求

——保证所提供的因特网信息服务业务的可用性、可恢复性达到一定的性能指标;

- 可用性:排除外力因素(非本企业可控制的因素),其业务可用性应 $\geq 99.95\%$,业务可用性是指用户能够使用本业务的时间占业务全部工作时间的百分数。95%以上的授权用户能够成功使用业务提供商所提供的信息服务业务,则该业务可用。
- 可恢复性:应支持在业务中断后,应在可接受的时间范围内(业务恢复时间间隔平均 $\leq 4h$,最长为 $8h^{(6)}$)恢复业务,且在最大程度上保护业务数据的完整性。

——对于提供电子邮件业务的增值电信业务网络,还应当拥有有效的机制防范因特网垃圾邮件,以保证正常用户邮件业务的使用。例如在邮件服务器中增加垃圾处理模块、设立专门人员和网络资源接受并及时处理用户对于垃圾邮件的投诉、引导用户在客户机中使用防范垃圾邮件的功能,详细要求参见YD/T 1311-2004《防范互联网垃圾电子邮件技术要求》。

B.2 信息内容合法性保障技术要求

提供信息服务业务的增值电信业务内容提供商应能够对于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。可以利用软件实施关键字过滤,也可以人工实时检查等。并应采用其他技术或人工手段有效防止其他类型(图像、音频、视频等)有害信息通过其业务网络向公众传播。

B.3 终端用户使用业务的安全保障措施技术要求

- 提供有效可靠的用户业务认证、授权和计费机制,防止未经授权的访问,保证业务顺利进行,计费信息准确。
- 应能够根据有关法律法规(《互联网信息服务管理办法》)的要求记录用户使用日志(从事新闻、出版以及电子公告等服务项目的互联网信息服务提供者,应当记录提供的信息内容及其发布时间、互联网地址或者域名),并且按有关法律法规(《互联网信息服务管理办法》)要求保留一定期限(至少60天)^⑥。

⑥ 参照《电信服务标准》中“因特网服务质量指标”项中有关通信设备障碍修复时限的数值。如果《电信服务标准》修订,则本标准应作相应改动。

⑦ 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。

附录C

(规范性附录)

国内多方通信服务安全保障要求

C.1 应用系统信息内容存储传输安全保障技术要求

1. 该类业务主要提供多点用户的音频或视频通信服务。提供该业务的增值电信业务网络应保证业务运营的可用性和可恢复性达到一定指标：
 - 可用性：排除外力因素（非本企业可控制的因素），其业务可用性应 $\geq 99.95\%$ 。业务可用性是指用户能够使用本业务的时间占业务全部工作时间的百分数。95%以上的授权用户能够成功使用业务提供商所提供的业务，则该业务可用。
 - 可恢复性：业务恢复时间间隔平均 $\leq 4h$ ，最长为8h。
2. 该业务对于用户数据的传输安全保证要求相对较低，因此无需提供特别的用户业务数据传输安全保障措施。
3. 对于该类业务中的国内因特网会议电视及图像服务业务，由于该业务中的某些应用具有向公众发布信息的属性，因此增值电信业务网络还应设置有效的检查机制保证向公众发布的各种信息（包括文本信息、多媒体信息、游戏内容）应符合我国法律法规（《互联网信息服务管理办法》）的规定。例如在网络游戏中，设置关键字过滤机制防止有害信息通过网络游戏在公众传播。

C.2 终端用户使用业务的安全保障技术要求

1. 为了保证业务不会被非法用户使用，提供该业务的增值电信业务网络还应提供用户接入认证与授权机制，例如接入口令设置，AAA协议等。
2. 提供该业务的增值电信业务网络还应具备业务安全审计能力，即应提供业务日志记录，并做一定期限（至少60天）的保存。

附录D

(规范性附录)

在线数据处理与交易处理业务安全保障要求

根据在线数据处理与交易处理业务定义,此类业务涉及金融、贸易等需要非常严格的安全保护的数据信息,因此其业务运营、信息内容、用户接入等方面的安全要求相比较其它业务都要严格。

D.1 应用系统信息内容安全保障措施技术要求

要使得该类涉及电子商务活动的业务安全运营,增值电信业务网络在进行本类增值业务运营时,应至少达到以下安全要求:

1. 业务可用性:排除外力因素(非本企业可控制的因素),其业务可用性应 $\geq 99.99\%$ 。业务可用性是指用户能够使用本业务的时间占业务全部工作时间的百分数。对于本类业务而言,99%以上的授权用户能够成功使用业务提供商所提供的业务,则该业务可用。
2. 业务资源保密性和完整性:业务网络应采用先进的加密和验证技术保证业务数据传输和存储安全。
3. 业务信息真实性:不可抵赖性是电子商务活动顺利进行并完成的重要方面。目前保证业务信息真实性的技术手段主要有数字签名技术。
4. 业务可恢复性:所有的业务数据应拥有可靠的备份,并且应支持在业务中断后,应在可接受的时间范围(业务恢复时间间隔平均 $\leq 4h$,最长为8h)内恢复业务,且业务数据不丢失。

要提供以上各项安全要求,可以采用某些综合性的安全技术和规范,例如在网络中应用IPSec协议保证网络传输的安全;提供采用业务加密和数字签名等口令服务所必需的密钥和证书管理等。目前我国已经出台了一系列电子商务行业标准和国家标准,例如:YD/T 1322.1-2004《电子商务技术要求 第一部分:基于扩充标记语言(XML)的企业对消费者(B2C)电子商务总体框架》等等。上面要求的各种安全技术的实施方法在这些标准中均有具体要求,因此要求增值电信业务运营商在实现这些安全技术时应参照相应的标准,尽可能保证在线数据处理与交易处理业务的网络和信息安全。

D.2 终端用户使用业务的安全保障措施技术要求

1. 提供在线数据处理与交易处理业务的增值电信业务网络应提供可靠的接入认证与授权机制,以保证使用业务的用户的合法性以及业务本身的安全性。
2. 提供在线数据处理与交易处理业务的增值电信业务网络应能够记录用户业务日志(包括详细的交易事件信息、操作步骤、时间等),并且应做永久或一定期限(至少3个月)的保存。

附录E

(规范性附录)

存储转发类业务安全保障要求

增值电信业务中的存储转发类业务目前都是采用X.25或者DDN专线网络承载,因此其业务系统受到的网络安全威胁相对较低。具体安全技术措施要求如下:

1. 该类业务的运营者应保证用户业务的可用性和可恢复性达到以下指标:
 - 可用性:排除外力因素(非本企业可控制的因素),其业务可用性应 $\geq 99.99\%$ 。业务可用性是指用户能够使用本业务的时间占业务全部工作时间的百分数。99%以上的授权用户能够成功使用业务提供商所提供的业务,则该业务可用。
 - 可恢复性:业务恢复时间间隔平均 $\leq 4\text{h}$,最长为8h。
2. 终端用户在使用存储转发类增值电信业务时,应用系统应提供用户接入认证与授权机制,例如接入口令设置等手段防止非法用户的接入。
3. 同时运营者还应提供准确的业务日志记录。
4. 在用户要求严格的数据安全保护情况下(例如加密传真、加密 X.400 电子邮件),还可以应用数据加密技术,保证用户数据在传送和存储时的安全。

附录F
(规范性附录)
IDC 业务安全保障要求

IDC业务安全具体要求待定。

附录G

(规范性附录)

国内因特网虚拟专用网业务安全保障要求

国内因特网虚拟专用网安全具体要求待定。

附录H
(规范性附录)
呼叫中心业务安全保障要求

呼叫中心业务的安全具体要求待定。

附录I
(资料性附录)
增值电信业务分类

1.1 第一类增值电信业务

1.1.1 在线数据处理与交易处理业务

在线数据与交易处理业务是指利用各种与通信网络相连的数据与交易/事务处理应用平台,通过通信网络为用户提供在线数据处理和交易/事务处理的业务。在线数据和交易处理业务包括交易处理业务、电子数据交换业务和网络/电子设备数据处理业务。

1.1.2 国内多方通信服务业务

国内多方通信服务业务是指通过通信网络实现国内两点或多点之间实时的交互式或点播式的语音、图像通信服务。国内多方通信服务业务包括国内多方电话服务业务、国内可视电话会议服务业务和国内因特网会议电视及图像服务业务等。

国内多方电话服务业务是指通过公用电话网把我国境内两点以上的多点电话终端连接起来,实现多点间实时双向语音通信的业务。

国内可视电话会议服务业务是通过公用电话网把我国境内两地或多个地点的可视电话会议终端连接起来,以可视方式召开会议,能够实时进行语音、图像和数据的双向通信。

国内因特网会议电视及图像服务业务是为国内用户在因特网上两点或多点之间提供的双向对称、交互式的多媒体应用或双向不对称、点播式图像的各种应用,如远程诊断、远程教学、协同工作、视频点播(VOD)、游戏等应用。

1.1.3 国内因特网虚拟专用网业务 (IP-VPN)

国内因特网虚拟专用网业务(IP-VPN)是指经营者利用自有的或租用公用因特网网络资源,采用TCP/IP协议,为国内用户定制因特网闭合用户群网络的服务。因特网虚拟专用网主要采用IP隧道等基于TCP/IP的技术组建,并提供一定的安全性和保密性,专网内可实现加密的透明分组传送。

1.1.4 因特网数据中心业务 (IDC)

因特网数据中心业务(IDC)是指利用相应的机房设施,以外包出租的方式为用户的服务器等因特网或其他网络的相关设备提供放置、代理维护、系统配置及管理服务,以及提供数据库系统或服务器等设备的出租及其存储空间的出租、通信线路和出口带宽的代理租用和其它应用服务。

1.2 第二类增值电信业务

1.2.1 存储转发类业务

存储转发类业务是指利用存储转发机制为用户提供信息发送的业务。语音信箱、X.400电子邮件、传真存储转发、语音邮件和增值传真存储转发业务属于存储转发类业务。

1. 语音信箱

语音信箱业务是指利用与公用电话网或公用数据传送网相连接的语音信箱系统向用户提供存储、提取、调用语音留言及其辅助功能的一种业务。每个语音信箱有一个专用信箱号码,用户可以通过终端设备,例如通过电话呼叫和话机按键进行操作,完成信息投递、接收、存储、删除、转发、通知等功能。

2. X.400电子邮件业务

X.400电子邮件业务是指符合ITU X.400建议、基于分组网的电子信箱业务。它通过计算机与公用电信网结合,利用存储转发方式为用户提供多种类型的信息交换。

3. 传真存储转发业务

传真存储转发业务是指在用户的传真机之间设立存储转发系统,用户间的传真经存储转发系统的控制,非实时地传送到对端的业务。

传真存储转发系统主要由传真工作站和传真存储转发信箱组成,两者之间通过分组网或数字专线连接。传真存储转发业务主要有:多址投送、定时投送、传真信箱、指定接收人通信、报文存档及其他辅助功能等。

1.2.2 呼叫中心业务

呼叫中心业务是指受企事业单位委托,利用与公用电话网或因特网连接的呼叫中心系统和数据库技术,经过信息采集、加工、存储等建立信息库,通过固定网、移动网或因特网等公众通信网络向用户提供有关该企事业单位的业务咨询、信息咨询和数据查询等服务。

呼叫中心业务还包括呼叫中心系统和话务员坐席的出租服务。

用户可以通过固定电话、传真、移动通信终端和计算机终端等多种方式进入系统,访问系统的数据库,以语音、传真、电子邮件、短消息等方式获取有关该企事业单位的信息咨询服务。

1.2.3 因特网接入服务业务 (ISP)

因特网接入服务是指利用接入服务器和相应的软硬件资源建立业务节点,并利用公用电信基础设施将业务节点与因特网骨干网相连接,为各类用户提供接入因特网的服务。用户可以利用公用电话网或其他接入手段连接到其业务节点,并通过该节点接入因特网。

因特网接入服务业务主要有两种应用,一是为因特网信息服务业务(ICP)经营者等利用因特网从事信息内容提供、网上交易、在线应用等提供接入因特网的服务;二是为普通上网用户等需要上网获得相关服务的用户提供接入因特网的服务。

1.2.4 信息服务业务

含电话信息服务(声讯服务)、因特网信息服务、和通信短消息服务、电子邮件。

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,通过固定网、移动网或因特网等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。

信息服务的类型主要包括内容服务、娱乐/游戏、商业信息和定位信息等服务。信息服务业务面向的用户可以是固定通信网络用户、移动通信网络用户、因特网用户或其他数据传送网络的用户。