ICS 35.040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 32906—2016

信息安全技术
中小电子商务企业信息安全建设指南

Information security technology—Guide of construction for information security in small & medium E-commerce enterprises

2016-08-29 发布　　2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本指导性技术文件按照 GB/T 1.1—2009 给出的规则起草。

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。

本指导性技术文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本指导性技术文件起草单位:浙江省标准化研究院、阿里巴巴(中国)有限公司、浙江工商大学、浙江经济信息中心、厦门标准化研究院、浙江科技学院、浙江飘飘龙网络科技有限公司、浙江富春江通信移动集团有限公司、北京天融信科技有限公司、上海天泰网络技术有限公司、中国计量学院。

本指导性技术文件主要起草人:李宁、刘璇、焦庆春、颜鹰、周广平、马骏、谢俊军、胡蓓姿、邵俊、刘若微、沈锡镛、陈宇、夏祖军、叶志强、范丙华等。

信息安全技术
中小电子商务企业信息安全建设指南

1 范围

本指导性技术文件给出了中小电子商务企业信息安全建设结构与模式、安全风险、安全需求、安全设计、安全实现与部署运管的指南。

本指导性技术文件适用于中小电子商务企业的信息安全建设，为电子商务项目开发、运行、维护提供技术参考。

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。

GB/T 20269 信息安全技术 信息系统安全管理要求

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 20988 信息安全技术 信息系统灾难恢复规范

GB/T 22081 信息技术 安全技术 信息安全管理实用规则

3 术语和定义

下列术语和定义适用于本文件。

3.1

中小电子商务企业 small & medium E-commerce enterprises

利用信息网络技术实现电子交易商务活动，每年电子交易单数在百万级以下的企业。

4 缩略语

下列缩略语适用于本文件。

CA：证书认证机构(Certificate Authority)

CPU：中央处理器(Central Processing Unit)

DDoS：分布式拒绝服务(Distributed Denial of service)

DES：数据加密标准(Data Encryption Standard)

ERP：企业资源计划(Enterprise Resource Planning)

HTTP：超文本传输协议(HyperText Transfer Protocol)

IDC：互联网数据中心(Internet Data Center)

IP：网络之间互连的协议(Internet Protocol)

IPsec：互联网安全协议(Internet Protocol Security)

PKI:公钥基础设施(Public Key Infrastructure)

SSH:安全外壳协议(Secure Shell)

SSL:安全套接层协议(Secure Sockets Layer)

URL:统一资源定位符(Uniform resource locator)

UPS:不间断电源(Uninterrupted power supply)

VPN:虚拟专用网络(Virtual Private Network)

VLAN:虚拟局域网(Virtual Local Area Network)

5 结构与模式

5.1 应用结构

中小电子商务企业信息安全应用结构如图1所示。

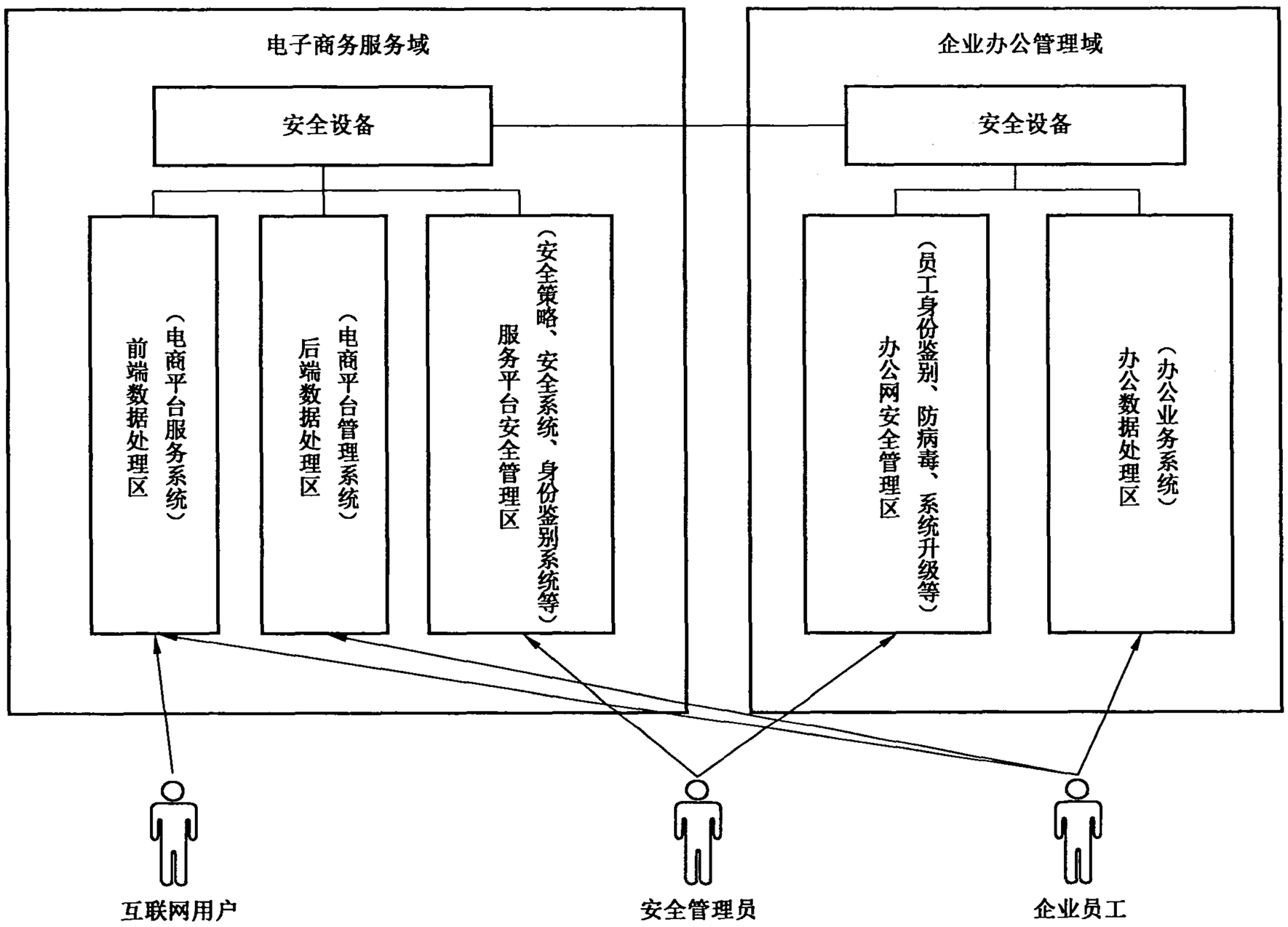

图1 中小电子商务企业信息安全应用结构图

中小电子商务企业信息安全应用结构主要包括:

a) 电子商务服务域是中小电子商务企业通过互联网向互联网用户提供电子商务服务的功能区域,包括前端数据处理区、后端数据处理区和服务平台安全管理区:

1) 前端数据处理区。与互联网用户交互的区域,包括用户信息发布、用户商品管理、用户注册、交易等公开信息的电子商务应用系统及其数据库,此区域可根据互联网用户授权后发布和修改其相应的信息内容等。前端数据处理区允许互联网用户授权访问。

2) 后端数据处理区。仅允许授权员工访问的区域,包括电子商务平台各种管理应用系统及其数据库,如商品管理系统、用户管理系统等。后端数据处理区仅允许员工授权访问。

3） 服务平台安全管理区。面向安全管理员的区域，包括为电子商务服务平台安全运行提供统一的资源管理、用户权限管理、认证管理等。服务平台安全管理区与办公网安全管理区只允许安全管理员访问。

b） 企业办公管理域是中小电子商务企业处理内部业务和办公的功能区域，包括办公数据处理区、办公网安全管理区：

1） 办公数据处理区。企业员工办公网区域，主要包括文件共享、人事系统、财务系统等办公管理需求及其数据库。办公数据处理区允许企业员工访问。

2） 办公网安全管理区。面向安全管理员的区域，包括员工权限管理、系统安全服务、网络安全管理服务等的区域。办公网安全管理区允许安全管理员访问。

c） 在电子商务服务域与企业办公管理域之间，通过信息安全设备，制定访问控制策略，防止非授权访问。

5.2 建设模式

5.2.1 概述

中小电子商务企业自行建设企业办公管理域内的相关信息安全措施，承担信息安全建设的所有风险责任；电子商务服务域的信息安全建设模式可分为自建模式、资源租用模式、店铺租用模式三类。

5.2.2 自建模式

中小电子商务企业依托电信运营商的互联网接入，自行建设所有互联网服务的物理设施与应用服务平台，对外提供电子商务服务。中小电子商务企业将承担信息安全建设的所有风险责任。

5.2.3 资源租用模式

资源租用模式包括：

a） 模式 1：物理资源租用。中小电子商务企业依托电信运营商和 IDC 提供的物理资源服务构建应用服务平台。中小电子商务企业承担主机安全、网络安全、应用安全与数据安全方面的风险责任，资源服务提供商承担物理安全方面的风险责任。

b） 模式 2：物理和主机资源租用。中小电子商务企业在依托电信运营商和 IDC 提供物理资源服务的基础上，租用资源服务商提供的系统主机构建应用服务平台。中小电子商务企业承担网络安全、应用安全与数据安全方面的风险责任，资源服务提供商承担物理安全和主机安全的风险责任。

c） 模式 3：物理、主机和网络服务资源租用。中小电子商务企业在依托电信运营商和 IDC 提供物理资源服务的基础上，租用资源服务商提供的系统主机与网络服务资源构建应用服务平台。中小电子商务企业承担应用安全与部分数据安全方面的风险责任，资源服务提供商承担物理安全、主机安全、网络安全和基础数据安全的风险责任。

5.2.4 店铺租用模式

以租用第三方电子商务平台提供的网上店铺资源，为消费者提供电子商务服务的模式。中小电子商务企业承担办公管理域内网络安全方面的风险责任，资源服务提供商承担物理安全、主机安全、应用安全与数据安全方面的风险责任。

根据不同的建设模式，电子商务服务域按表 1 选择安全建设项目，结构参见附录 A。

表 1　电子商务服务域安全建设要求表

安全项目	建设模式				
	自建模式	资源租用模式			店铺租用模式
		模式 1:物理资源租用	模式 2:物理和主机资源租用	模式 3:物理、主机和网络服务资源租用	
物理安全	√	—	—	—	—
主机安全	√	√	—	—	—
网络安全	√	√	√	○	○
应用安全	√	√	√	√	—
数据安全	√	√	√	○	○
注:“√”由中小电子商务企业承担;“—”由资源租赁方承担;“○”由中小电子商务企业与资源租赁方根据电子商务应用结构分别承担相应责任。					

5.3　建设流程

中小电子商务企业信息安全建设流程可划分为信息安全风险评估、需求分析、方案设计、安全实现、部署运管等阶段。

6　安全风险

6.1　物理风险

中小电子商务企业面临的物理安全风险主要包括但不限于:电子商务服务域内的非法进入、盗窃、破坏、雷击、失火、异常温湿度和断电等情况,企业办公管理域内的非法进入、盗窃等情况,可能会导致设备损坏、数据丢失、泄密等后果。

6.2　网络风险

中小电子商务企业面临的网络安全风险主要包括但不限于:电子商务服务域内的非授权访问、网络攻击和网络设备入侵等情况,企业办公管理域内的非授权访问、网络设备入侵等情况,可能会导致拒绝服务、隐私泄露等后果。

6.3　主机风险

中小电子商务企业面临的主机安全风险包括但不限于:电子商务服务域内的非法登录、权限划分不正确、系统漏洞和恶意代码等情况,企业办公管理域内的系统漏洞和恶意代码等情况,可能会导致非法入侵、信息泄密等后果。

6.4　数据风险

中小电子商务企业面临的数据安全风险主要包括但不限于:电子商务服务域内的传输出错、数据丢失等情况,企业办公管理域内的数据丢失、备份出错等情况,可能会导致数据的丢失和泄露等后果。

6.5 应用风险

中小电子商务企业面临的应用安全风险主要包括但不限于：电子商务服务域内的身份冒用、授权过度和通信欺骗等情况，企业办公管理域内的身份冒用、授权过度等情况，可能会导致数据篡改、越权访问、信息泄密等后果。

7 安全需求

中小电子商务企业应对信息安全风险，具有信息安全防护的需求，主要涉及物理安全、网络安全、主机安全、数据安全和应用安全等方面，包括但不限于以下内容：

a) 关键设备使用区的进入许可、防盗窃、防破坏、防雷击、防火、温湿度控制和持续供电等需求。

b) 计算机网络控制方面的访问控制、入侵防范和网络设备防护等需求。

c) 计算机主机管理和访问的身份鉴别、权限控制、入侵防范和恶意代码防范等需求。

d) 电子商务数据保护方面的数据完整性检测、数据保密、数据备份和恢复等需求。

e) 电子商务应用的身份鉴别、交易安全和通信保护等需求。

8 安全设计

8.1 一般原则

中小电子商务企业信息安全设计应遵循以下原则：

a) 安全设计和相关安全产品应符合国家有关法律法规和标准要求。

b) 安全设计应区分不同建设模式，满足相对应的安全需求。

8.2 安全结构

中小电子商务企业的信息安全建设宜依托物理安全，构建网络安全、主机安全、数据安全与应用安全，同时结合信息安全管理和运营风险控制形成整体信息安全结构，如图 2 所示。

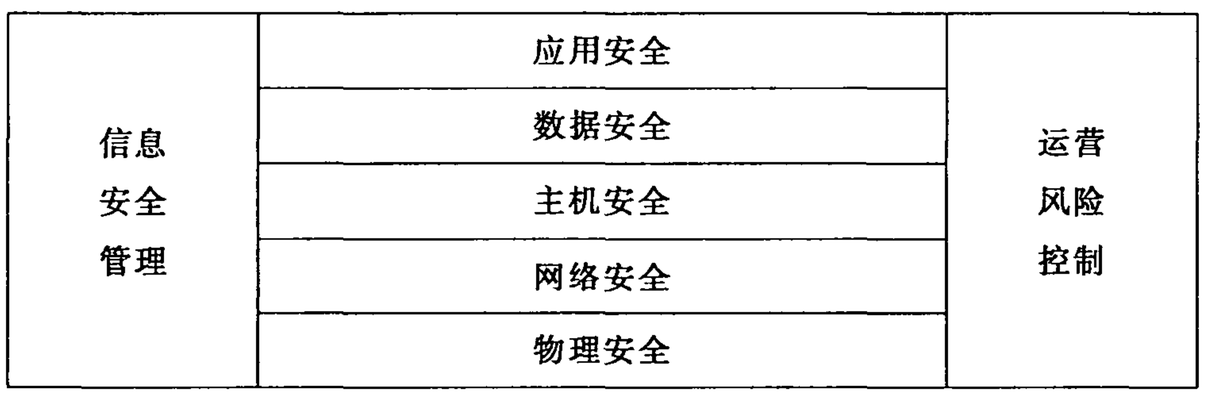

图 2 中小电子商务企业电子商务安全结构图

8.3 物理安全设计要求

物理安全设计要求包括但不限于：

a) 关键设备使用区域出入口能对进出人员实现控制与记录。

b) 主要设备有标识标记并具有防盗等管理措施。

c) 良好接地与相关避雷措施能满足主要设备的防护要求。

d) 火灾探测与灭火措施应能覆盖主要设备使用区域。

e) 关键设备使用区域的温湿度环境能符合设备运行要求。

f) 电源质量能符合关键设备的运行要求，在断电情况下应有安全措施满足其连续运行。

8.4 网络安全设计要求

网络安全设计要求包括但不限于：

a) 在边界上针对网络数据流入/流出提供过滤和保护，通过网络手段阻断特定内外连接。

b) 可按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。

c) 可在网络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、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。

d) 可采用相关措施保证网络设备用户身份的合法性和唯一性。

e) 可对网络设备的管理员登录地址进行限制。

f) 可采用相关措施保证身份鉴别信息不易被冒用，口令具有复杂度和时效性。

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

8.5 主机安全设计要求

主机安全设计要求包括但不限于：

a) 可采用相关措施保证操作系统和数据库系统的用户身份的合法性。

b) 可启用访问控制功能，依据安全策略控制用户对资源的访问。

c) 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，并通过设置升级服务器等方式保持系统补丁及时得到更新。

d) 可部署防恶意代码相关工具，并保持使用工具的有效性的可用性。

e) 可采用相关措施具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。

8.6 数据安全设计要求

数据安全设计要求包括但不限于：

a) 能够检测到鉴别信息和重要业务数据在传输过程中完整性受到破坏。

b) 可采用加密或其他保护措施实现鉴别信息的存储保密性。

c) 可能够对重要信息进行备份和恢复。

8.7 应用安全设计要求

应用安全设计要求包括但不限于：

a) 可采用相关措施保证登录用户身份的合法性。

b) 宜支持交易数据在传输过程或存储中不被未授权实体获得，保证数据机密。

c) 宜支持交易数据不能在未经授权的情况下进行任何的更改，保证数据完整。

d) 宜具有可验证的电子凭证，支持客户和商家均不能否认已达成的交易，保证交易过程抗抵赖。

e) 宜支持交易买家身份的识别，保证交易方可追溯。

9 安全实现

9.1 物理安全实现

9.1.1 概述

企业办公管理域的物理安全由中小电子商务企业自行建设，电子商务服务域的物理安全可根据不

同模式进行建设。

采用自建模式的物理安全由中小电子商务企业自行建设;采用店铺租用模式和资源租用模式的物理安全由服务提供商负责建设。

9.1.2 物理安全措施

物理安全实现包括但不限于以下措施:

a) 将主要设备放置在机房内,将设备或主要部件进行固定,并设置明显的不易除去的标记。

b) 设置温湿度调节与监控设施。

c) 机房出入安排专人负责,控制鉴别和记录出入信息,可配置电子门禁、入侵报警、视频监控等安防系统。

d) 机房设置火灾自动报警系统和灭火设备。

e) 机房设置避雷装置,供电线路配置稳压器和过电压防护设备,使用不间断电源。

9.2 网络安全实现

9.2.1 概述

网络安全主要包括电子商务服务域、企业办公管理域以及网络边界的安全防护。

企业办公管理域的网络安全实现由中小电子商务企业自行建设,电子商务服务域的网络安全实现根据不同建设模式区分相关责任主体:

a) 自建模式的中小电子商务企业需对所有区域及边界进行网络安全防护措施建设。

b) 资源租用模式的中小电子商务企业根据租用模式由服务提供商和/或企业负责建设网络安全措施。

c) 店铺租用模式的资源提供方应建设电子商务服务域及边界的所有网络安全防护措施。

9.2.2 访问控制实现

可在网络边界部署访问控制设备,启用访问控制功能,包括但不限于以下措施:

a) 可使用包过滤防火墙:可支持基于 IP 地址的访问控制、端口的访问控制、协议类型的访问控制;可支持 HTTP、FTP、POP3、SMTP 等协议的应用代理;可根据 IP 地址、协议、时间等参数对流量进行统计;具有完整的日志记录和良好的日志分析能力;可进行安全域设定并对各安全域之间的访问进行控制。

b) 可使用安全路由器:通过内置防火墙、IPsec 等模块,提供网络互连、流量控制、网络和信息安全维护等安全功能,阻止安全域外部连接进入内部,保障网络通信的安全性。

c) 可使用安全交换机:通过基于 ACL 的报文过滤、CPU 过载保护、广播风暴控制、VLAN、基于 802.1X 的接入控制、交换机与 IDS 系统的联动等安全功能,保障安全域数据交换的安全性。

9.2.3 入侵防范

入侵防范包括但不限于以下措施:

a) 使用入侵检测和防御系统,可在网络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、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) 使用网络活动监测工具,当检测到攻击行为时,可记录攻击源 IP、攻击类型、攻击目的、攻击时间,在发生严重入侵事件时能提供报警及自动采取相应动作。

c) 可使用安全网关,防止病毒传播和网际恶意代码攻击。

9.2.4 网络设备防护

网络设备防护包括但不限于以下措施：

a) 采用终端接入控制，对接入系统的终端进行访问控制，发现终端接入系统的行为，并根据访问控制策略采取行动(如允许授权终端接入、断开非授权的终端连接等)，通过对终端接入的控制，保障安全域边界安全。

b) 保护终端使用安全，对接入系统的终端进行保护，防止对终端的未授权使用(如终端使用口令保护等)，通过对终端的保护，保障安全域边界安全。

9.2.5 安全审计

可采用网络安全审计系统，实现网络安全审计，包括但不限于以下措施：

a) 可对网络系统中的网络设备运行状况、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。

c) 可根据记录数据进行分析，并生成审计报表。

d) 可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。

e) 可定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施，当存储空间被耗尽时，终止可审计事件的发生。

f) 可根据信息系统的统一安全策略，实现集中审计，时钟保持与时钟服务器同步。

9.3 主机安全实现

9.3.1 概述

主机安全主要是为企业办公终端、服务器主机或单机用户提供基于单个主机的操作安全、访问控制、入侵和恶意代码防范等综合安全防护措施，具体可参见附录 B。

企业办公管理域的主机安全实现由中小电子商务企业自行建设，电子商务服务域的主机安全实现根据不同建设模式区分相关责任主体：

a) 自建模式的中小电子商务企业需进行主机安全措施建设。

b) 资源租用模式的主机安全根据租用模式由服务提供商和/或企业负责建设主机安全措施。

c) 店铺租用模式的主机安全由服务提供商建设主机安全措施。

9.3.2 单机防火墙

设置单机防火墙可采用但不限于以下措施：

a) 对进出终端数据包进行安全过滤。

b) 实现统一策略下发到终端，启用操作系统自带防火墙功能。

9.3.3 主机访问控制

主机访问控制可采用但不限于以下措施：

a) 启用访问控制功能，依据安全策略控制用户对资源的访问。

b) 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) 及时删除多余的、过期的账户，避免共享账户的存在。

9.3.4 主机身份鉴别

主机身份鉴别可采用但不限于以下措施：

a) 设置域账号服务器对用户登录操作进行身份标识和鉴别。
b) 设置 VPN 账号服务器对 VPN 用户接入身份标识和鉴别。
c) 各类服务器的所有账号均需设置口令,符合复杂度要求。
d) 启用登录失败处理功能,设定账户锁定阈值和账户锁定时间。
e) 采用加密传输的远程桌面管理工具管理服务器。
f) 域账号、VPN 账号的设置均需要唯一性,以便追溯到用户。

9.3.5 主机入侵防范

主机入侵防范可采用但不限于以下措施:

a) 检测对重要服务器进行入侵的行为,能够记录入侵的源 IP、攻击类型、攻击目的、攻击时间,并在发生严重入侵事件时提供报警。
b) 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。
c) 操作系统遵循最小安装的原则,仅安装需要的组件和应用程序,并通过设置升级服务器等方式保持系统补丁及时得到更新。

9.3.6 主机恶意代码防范

主机恶意代码防范可采用但不限于以下措施:

a) 安装防恶意代码工具,并及时更新防恶意代码工具版本和恶意代码库。
b) 主机防恶意代码工具具有与网络防恶意代码工具不同的恶意代码库。
c) 支持防恶意代码的统一管理。

9.3.7 主机安全审计

主机安全审计可采用但不限于以下措施:

a) 启用主机审计功能,覆盖对账户登录事件、账户管理、目录服务访问、登录事件、对像访问、策略更改、系统事件等类型的审核记录。
b) 定期查看和备份审计记录。

9.4 数据安全实现

9.4.1 概述

自建模式和资源租用模式自行开发应用,需进行数据安全建设。店铺租用模式采用服务提供商的应用,数据安全由服务提供商负责。

9.4.2 数据完整性检测

可部署检测系统对管理数据、鉴别信息和重要业务数据在传输过程中数据是否被破坏的完整性进行检测,并在检测到完整性错误时采取必要的恢复措施。

9.4.3 数据备份系统

数据备份是保护数据安全的手段,可部署数据备份系统,宜实现但不限于以下功能:

a) 备份集中管理,同步支持服务器数据和客户机数据的备份和恢复。
b) 数据格式开放,兼容多种数据存储设备。
c) 数据备份系统可支持多种计算机软件硬件系统主平台。
d) 数据备份系统可支持异构网络,支持 SNMP 网管协议,接受网管系统的监视。

9.4.4 灾难恢复

此项可按 GB/T 20988 的要求进行实施。

9.5 应用安全实现

9.5.1 概述

自建模式和资源租用模式自行开发应用，需进行应用安全建设。店铺租用模式采用服务提供商的应用，应用安全由服务提供商负责。

9.5.2 身份鉴别安全实现

9.5.2.1 概述

身份鉴别主要是保证互联网用户及企业员工的用户信息安全，是电子商务信息安全的基础，可包括用户安全管理、数字签名技术、数字时间戳技术、数字证书等。店铺租用模式和资源租用模式的中小电子商务企业用户直接采用电子商务平台服务商提供的身份鉴别系统，认证体系安全由服务提供商负责；自建模式的中小电子商务企业可自建认证系统，也可采用第三方 CA 认证机构。

提供身份验证的第三方 CA 认证机构，可由一个或多个用户信任的组织实体构成，实现电子商务活动中交易参与各方身份、资信的认定，维护交易活动的安全。

9.5.2.2 用户安全管理

用户信息安全管理可启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

9.5.2.3 数字签名技术

保证信息传输过程中信息的完整性和信息发送者的身份鉴别和抗抵赖性可采用数字签名技术，宜实现但不限于以下功能：

a) 由签名者随信息发出，与信息不可分离。

b) 签名随信息内容改变而不同，可确认信息自发出至接收未做过任何修改。

9.5.2.4 数字时间戳技术

提供对电子文件发表、签订的时间内容的安全保护，保证文件符合交易时间要求，宜实现但不限于以下内容：

a) 需加时间戳的文件的摘要。

b) 收到文件的日期和时间。

c) 数字时间戳的数字签名。

9.5.2.5 数字证书

用户的数字证书是 PKI 执行机构 CA 所颁发的核心元素，符合 GB/T 20518 的要求，宜实现但不限于以下功能：

a) 管理签名用户证书的密钥和其他密钥的产生、更新、备份、恢复等。

b) 接收用户的证书请求，审核用户的合法身份，发放用户的数字证书，管理用户的证书等。

c) 黑名单管理，包括注销用户的数字证书、定期产生黑名单、发布黑名单。

d) 目录管理，目录服务器设置、证书、CRL(证书撤销列表)等的更新等。

9.5.3 交易安全实现

9.5.3.1 概述

交易安全包括数据接入安全、交易服务、Web 服务和 SSL 等。店铺租用模式的中小电子商务企业用户直接采用电子商务平台服务商提供的安全交易服务，交易安全由服务提供商负责；资源租用模式和自建模式的交易安全由中小电子商务企业自行负责建设。

9.5.3.2 互联网服务

互联网服务宜采取但不限于以下措施：

a) 支持权限拥有者把权限授权给其他实体，实体可进行一些安全操作，如网页访问、网页数据修改、删除等。
b) 支持未授权用户不能访问互联网服务器及客户端与服务器之间的保密信息。
c) 支持互联网数据在未经授权的情况下不能被删除或更改。
d) 支持授权用户能在授权范围内的活动。
e) 支持互联网漏洞修复。

9.5.3.3 交易服务

中小电子商务交易服务在通信双方建立连接之前，应用系统可利用密码技术进行会话初始化验证；可对通信过程中的敏感信息字段进行加密；可采用校验码技术保证通信过程中数据的完整性。

9.5.3.4 数据接入安全

外部数据接入安全宜采取但不限于以下措施：

a) 与外部合作方签订相关合作与安全协议。
b) 对合作方 URL 进行监控。
c) 接口以 HTTP 方式开放。
d) 设计接口有身份鉴别，并对来源授权。
e) 接口调用有日志记录。
f) 参数传递做签名验证，并应有时间戳。
g) 明确用户上传的文件类型。
h) 对用户上传的图片，进行服务端安全处理。

9.5.3.5 数据传输安全

数据传输安全宜采取但不限于以下措施：

a) 在客户端与服务器之间建立安全的通道，可使用 SSL 对数据进行处理。
b) 为确保用户的合法性，可在握手交换过程中采用数字认证。
c) 为保证数据的机密性，可采用 DES 等加密算法。

10 部署运管

10.1 部署安装

在电子商务系统安装部署时，采取相应措施确保系统安全功能的实现，对操作系统、数据库、应用系统等软件的安装部署和配置应该符合相应的安全规范和标准。

10.2 文档评估审查

在电子商务系统投产前进行安全评估或审查，通过审查系统设计文档中的安全功能设计、系统测试文档中的安全功能测试，确保系统本身安全功能的实现。通过审核系统安装与配置过程或文档，确保系统安全配置的落实与实现。

10.3 安全测试

10.3.1 安全测试要求

在电子商务系统测试阶段，根据电子商务系统安全功能要求进行测试，确保所有设计的安全功能要求均能得到实现。在测试报告或相关文档中应明确说明检查列表中各项安全功能要求的实现情况。

10.3.2 测试过程安全管理

在电子商务系统开发测试过程中，对于数据要根据相关规定进行变形处理，禁止在开发或测试环境中直接使用生产系统的密钥和用户密码等重要数据。测试环境要依据相关规定进行合适的管理和安全防护，并通过相应的手段确保与生产系统、开发系统隔离。

10.4 投入运行

电子商务系统投入正式运行前，需清除系统中各种临时数据，进行管理权交接，开发方不得随意更改安全策略和系统配置。

10.5 安全管理

10.5.1 总体要求

总体要求参照 GB/T 22081、GB/T 20269 中的相关要求。

10.5.2 安全策略

安全策略宜采用但不限于以下措施：

a) 管理层制定清晰的策略方向，策略文档说明管理承诺，并提出管理信息安全的途径。
b) 对涉及整个电子商务系统安全的关键策略要由管理层批准，进行统一管理，同时建立策略变更审批制度。
c) 在整个组织中颁发和维护信息安全策略。

10.5.3 机构和人员管理

机构和人员管理宜采用但不限于以下措施：

a) 严格选拔网上交易人员，落实工作责任制。
b) 建立信息安全专职管理队伍，配备足够的安全管理人员，信息安全管理人员需经过安全培训才能上岗。
c) 实施信息安全意识的培训教育和安全技术培训。

10.5.4 安全管理制度

安全管理制度宜采用但不限于以下措施：

a) 建立电子商务系统网络、系统、应用等各层面的安全管理制度。包括对信息系统规划、建设、运行、维护各个阶段的安全管理。

b) 建立网络系统的日常维护制度。日常维护包括网络设备、服务器和客户机、通信线路、支撑软件、应用软件等日常管理和维护。

c) 建立病毒防范制度。病毒防范包括安装计算机防病毒软件，认真执行病毒定期清理制度，控制权限，高度警惕网络陷阱等。

10.5.5 安全跟踪管理

建立电子商务系统日志机制，用来记录系统运行的全过程。包括建立安全保护技术措施，保留用户注册信息以及修改历史记录，保留用户登录(登录时间、登录 IP)、信息发布等日志信息，保留交易列表、交互信息及交互对象用户列表等。

10.5.6 信息安全审核管理

有信息审核制度，对在所提供服务范围内的用户发布的信息进行逐条审核，实行先审后发等措施，包括但不限于：经常对系统日志进行检查和审核，及时发现系统故意入侵行为和违反系统安全功能的记录，监控和捕捉各种安全事件，保存、维护和管理系统日志。

10.5.7 应急措施管理

系统运行可能会因为自然或人为的原因遭破坏，制定相应问题处理的应急方案，主要包括系统备份和系统恢复以及法律证据收集等。系统定期对数据进行完全备份，定期建立包括应用系统以及操作系统等在内的完整镜像，同时定期对数据做增量备份。具体可参照附录 C。

10.6 运营风险控制管理

中小电子商务企业在开展电子商务时，可根据相关管理要求进行交易欺诈、隐私保护等风险控制管理。

附 录 A
（资料性附录）
典型模式结构图

A.1 自建模式结构

图 A.1 给出了中小电子商务企业自建模式结构图。

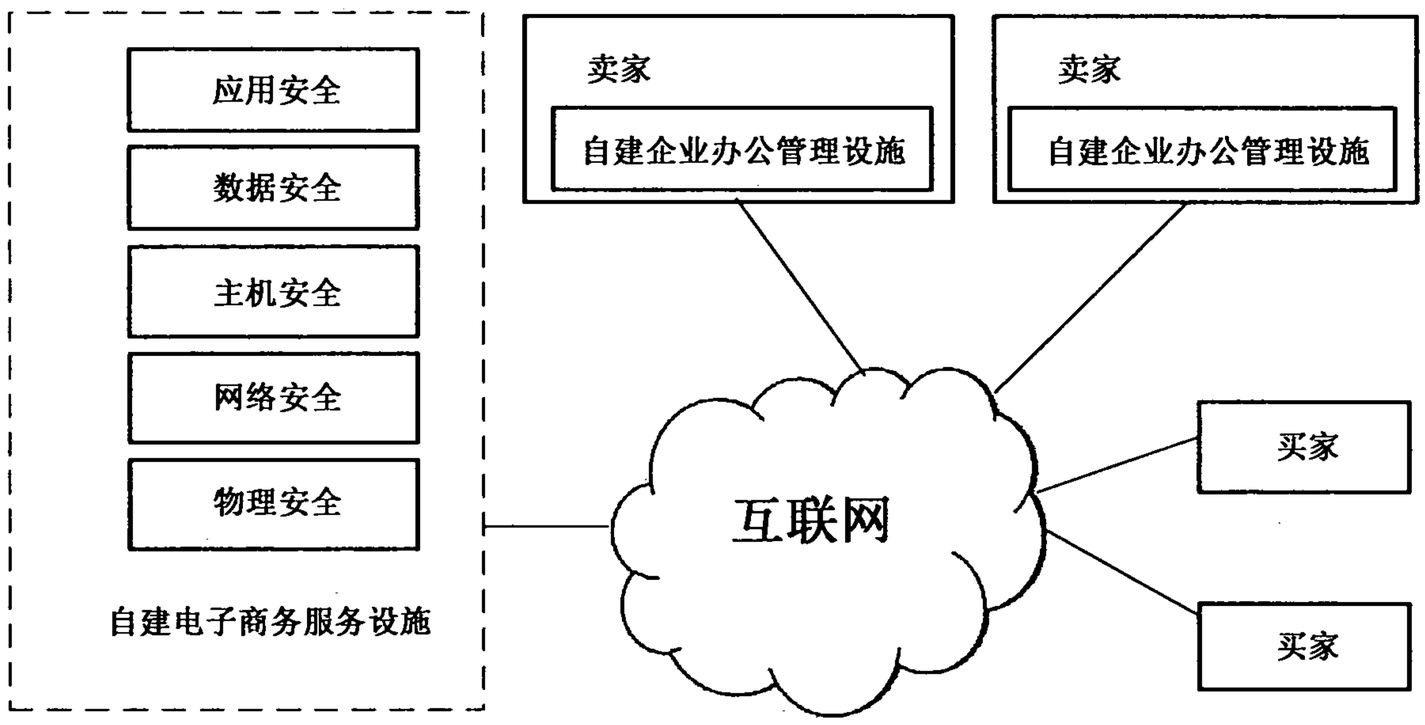

图 A.1 中小电子商务企业自建模式结构图

自建模式包括整个硬件和软件建设，及其相应的安全建设管理。自建模式可以给其他电子商务卖家提供服务或者给买家消费者提供服务。

A.2 资源租用模式结构

图 A.2 给出了中小电子商务企业资源租用模式 1 结构图。

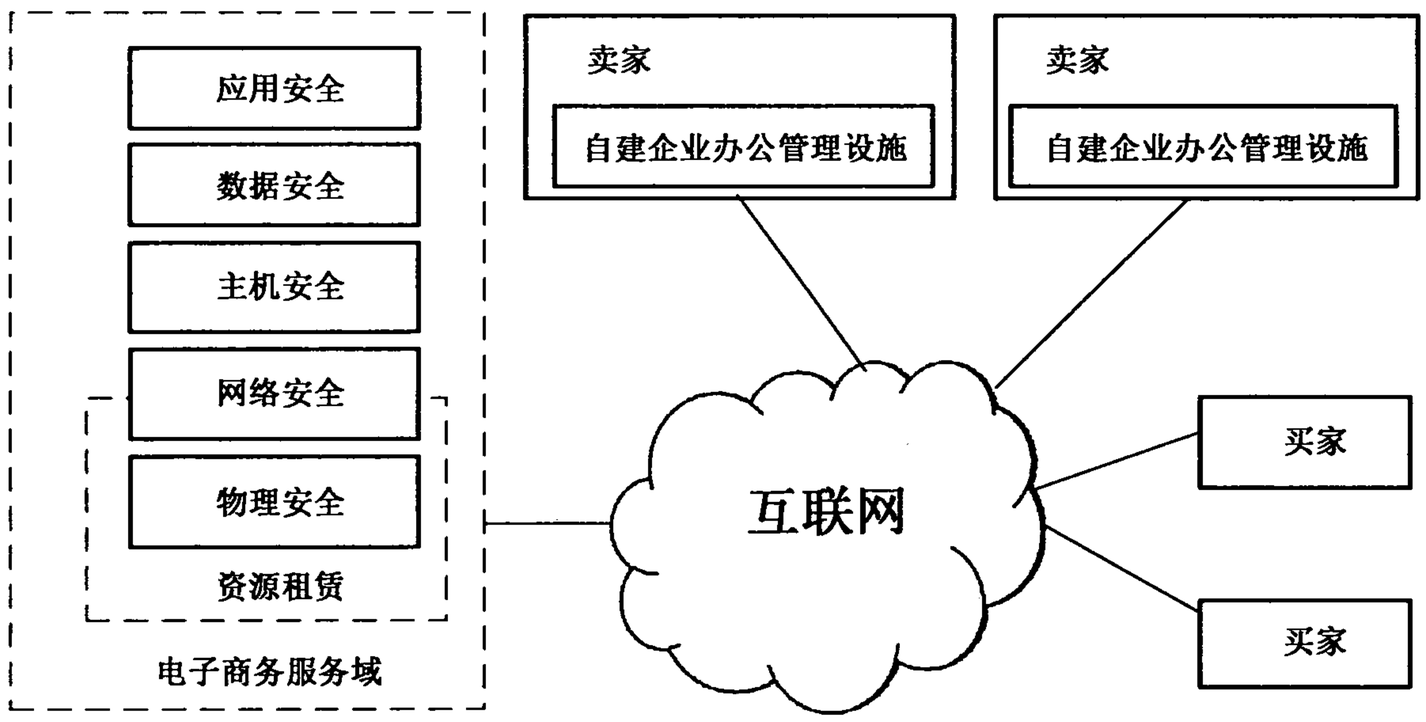

图 A.2 中小电子商务企业资源租用模式 1 结构图

图 A.3 给出了中小电子商务企业资源租用模式 2 结构图。

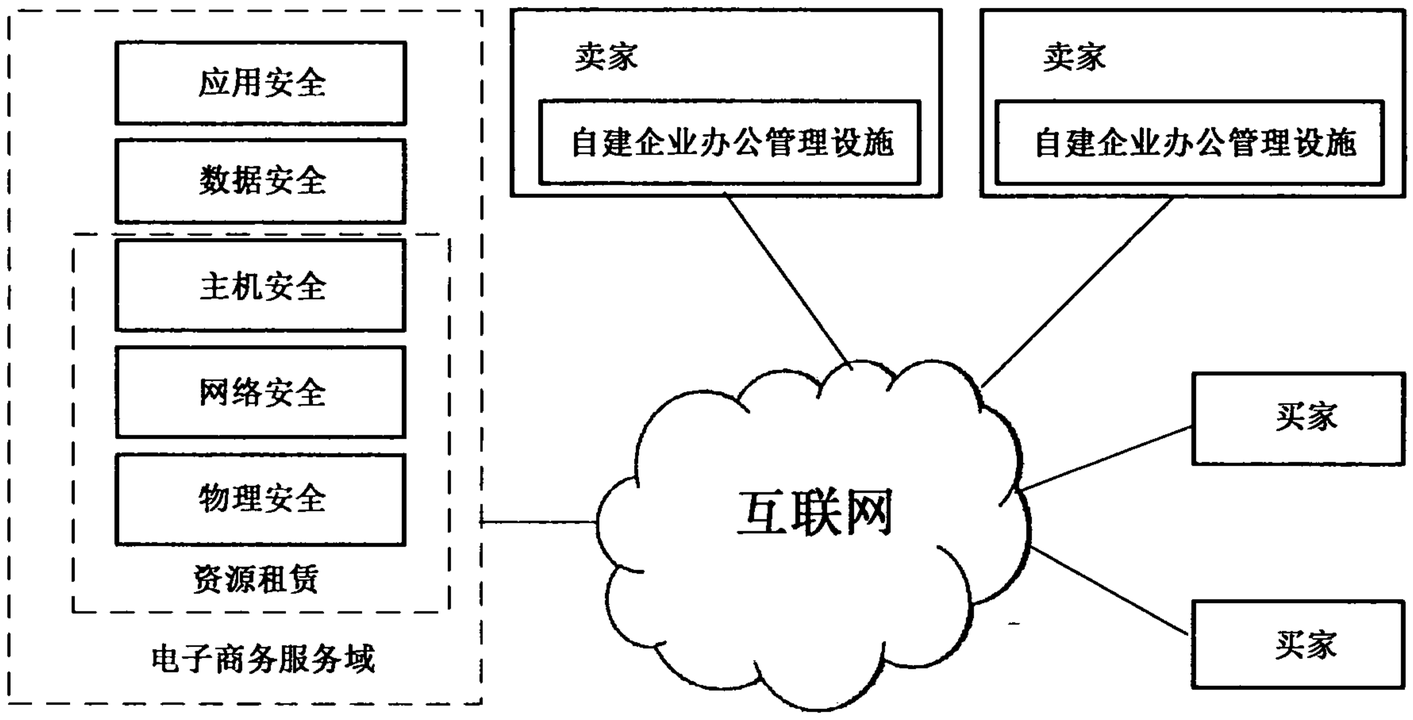

图 A.3　中小电子商务企业资源租用模式 2 结构图

图 A.4 给出了中小电子商务企业资源租用模式 3 结构图。

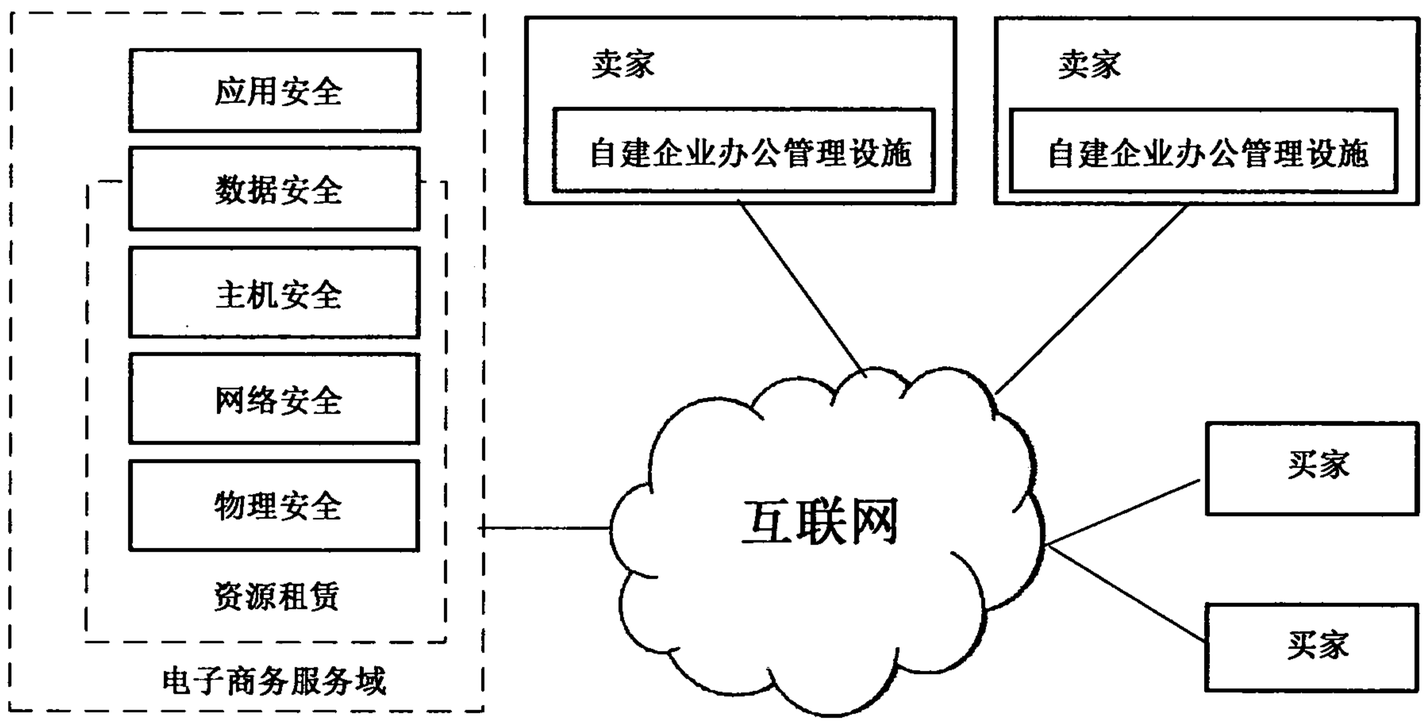

图 A.4　中小电子商务企业资源租用模式 3 结构图

资源租用模式主要包括软件建设及局域网内安全。资源租赁模式可以给其他电子商务卖家提供服务或者给买家消费者提供服务。

A.3　店铺租用模式结构

图 A.5 给出了电子商务店铺租用模式结构图。

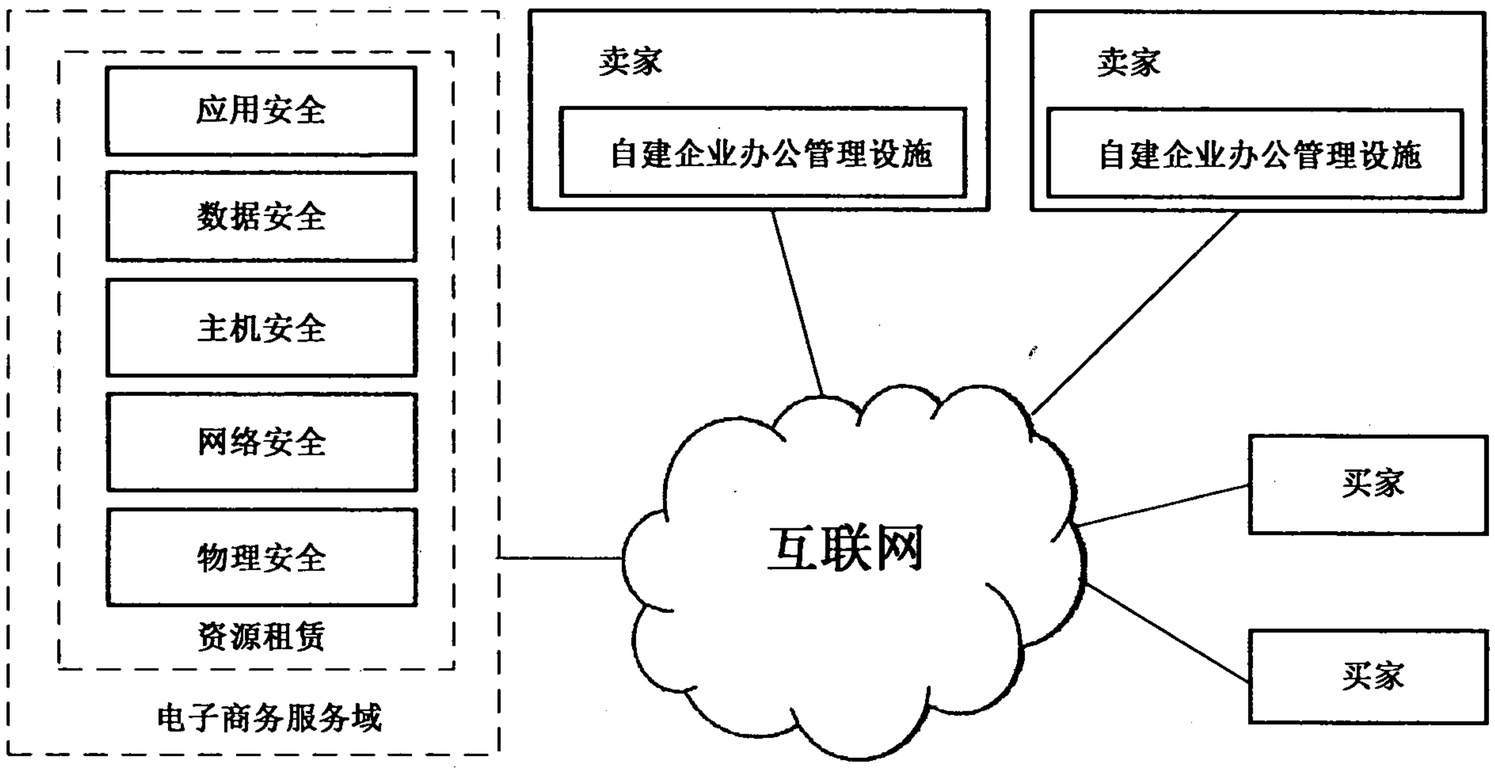

图 A.5　中小电子商务企业店铺租用模式结构

店铺租用模式的信息安全建设由电子商务平台服务商提供。店铺租用模式通过电子商务平台向消费者提供电子商务服务。

附 录 B
（资料性附录）
中小电子商务企业信息安全自建模式案例

B.1 某电子商务企业电子商务服务域信息安全建设

B.1.1 机房物理安全

B.1.1.1 机房选址

满足如下基本要求：

a） 机房选择具有防震、防雨和防风能力的建筑物。

b） 机房场地禁止设在在建筑物地下或顶层。

B.1.1.2 物理访问控制

满足如下基本要求：

a） 机房所在建筑物及机房入口均 24 h 专人值守。

b） 除机房管理人员外的人员来访均需机房管理员授权。

c） 来访人员均进行身份核查并登记，进出机房要机房管理员全程陪同。

d） 采用物理隔断对机房内各区域进行划分，在机房重要区域前设置电子门禁。

e） 保留电子门禁的运行和维护记录。

B.1.1.3 防盗窃和防破坏

满足如下基本要求：

a） 机房所有设备均需要放置于机架上并固定，机架、设备、线缆均需标识资产标签。

b） 机房内线缆均采用下走线，用于备份的磁带、硬盘等存储介质需要分类标识并放置于专用柜中，机房内需配备防盗报警并保留运行和维护记录。

c） 机房内需要设置无盲区 24 h 视频监控，视频监控信息需保留 3 个月，视频监控信息支持实时查看，视频探头、监控记录需定期检查。

B.1.1.4 防雷击

满足如下基本要求：

a） 机房所在建筑物安装防雷保安器防止感应雷。

b） 机房设置交流底线。

B.1.1.5 防火

满足如下基本要求：

a） 机房设置自动气体灭火装置。

b） 自动气体灭火装置具备自动检测火情和自动报警功能。

c） 机房工作间和辅助房均采用 A1、A2 级别的耐火等级建筑材料。

d） 机房可采用铁笼隔离将重要设备与其他设备隔离。

B.1.1.6 防水和防潮

满足如下基本要求：

a) 机房房顶上、活动地板下不得有水管穿过。

b) 机房采用监控系统对温湿度进行监控和报警。

c) 机房应设置挡水和排水设施。

d) 定期检查机房湿度并保留记录。

B.1.1.7 防静电

满足如下基本要求：

a) 机房采用静电地板。

b) 机房内所有机柜均采用防静电措施。

B.1.1.8 温湿度控制

满足如下基本要求：

a) 机房采用精密空调将机房温度控制在 23 ℃±3 ℃，湿度 40%～55%并保持空调系统 7×24 h 工作正常。

b) 机房维护人员每 2 h 巡检一次温湿度。

B.1.1.9 电力供应

满足如下基本要求：

a) 机房内采用具有稳压功能的 UPS，UPS 备用电力至少支撑 2 h。

b) 机房内设置并行电缆线路为机房供电。

c) 机房配备柴油发电机并能在 UPS 电力短缺时自动切换，机房可考虑建立油库或同附件加油站签署供油协议。

d) 机房维护人员每 2 h 巡检一次供电系统。

B.1.1.10 电磁防护

满足如下基本要求：

a) 机房电源线和通信线缆需要隔离铺设。

b) 机房内采用接地方式防止外界电磁干扰和设备寄生耦合干扰。

B.1.2 网络安全

B.1.2.1 网络安全域的划分

满足如下基本要求：

a) 按照电子商务服务域的安全需求，可划分为互联网接入区、前端应用接入区、后端管理接入区三个安全域。

b) 安全域描述(见表 B.1)。

表 B.1　电子商务服务域网络安全域描述

安全域	描述
互联网接入区	用于外部互联网络接入
前端应用接入区	用于网站前台、支付系统、商品系统、业务流程管理、信息展示、安全保障系统前端等面向互联网用户的系统接入
后端管理接入区	用于会员管理、权限管理、系统配置系统、数据库系统、安全保障系统后端，办公管理端通过 VPN 接入

B.1.2.2　网络结构

满足如下基本要求：

a)　对核心层、汇聚层网络设备考虑硬件冗余。

b)　互联网接入保证足够带宽以满足互联网用户的需求。

c)　根据各安全域内系统的重要性，采用 VLAN 技术划分不同的子网或网段，通过路由协议认证建立安全的访问路径。

d)　在核心层网络设备上提供带宽优先级分配，保障重要业务的带宽。

B.1.2.3　访问控制

满足如下基本要求：

a)　通过路由器控制互联网接入区对前端应用区、后端管理区和办公管理端的访问，核心交换机控制前端应用接入区和后端管理区之间的访问，汇聚交换机控制后端管理区内各管理系统和数据库之间的访问。

b)　各安全域采用访问控制列表技术实现源、目的地址的端口级访问控制。

c)　关闭不必要的协议端口。

d)　通过设置负载均衡设备控制网络会话数连接。

e)　建立网络流量负载检测和扩容机制。

f)　对前端应用区、后端管理区交换机配置 IP、MAC(消息鉴别码)地址绑定。

g)　采用 VPN 技术提供办公管理端对后端管理区的接入。

B.1.2.4　边界完整性检查

满足如下基本要求：

a)　采用安全域和 802.1X 认证结合技术控制外部用户网络接入和网络访问去向控制。

b)　互联网接入区只允许外部访问前端应用区 80 和 443 端口，前端服务区和后端管理区采用访问控制列表的方式控制内部用户对外网的访问。

B.1.2.5　入侵防范

部署网络流量侦测设备，对符合 DDoS 攻击行为的异常流量予以清洗或路由黑洞。

B.1.2.6　安全审计

满足如下基本要求：

a)　设置专用的 syslog 日志服务器收集和存储网络设备日志并对日志进行分析形成图表报告。

b) 设置第三方审计系统进行审计，审计记录包括日期、时间、用户/IP、事件类型、信息描述等。

B.1.2.7 网络设备防护

满足如下基本要求：

a) 采用用户名＋口令的方式对登录网络设备的用户进行身份鉴别，vty 和 console 登录需要 tacacs 服务器认证。
b) 采用绑定堡垒机 IP 的方式限制对网络设备的登录。
c) 登录 tacacs 服务器的用户名具有唯一性。
d) 网络设备的登录需要管理员 pin 码和动态令牌登录到堡垒机。
e) 堡垒机登录失败 3 次后自动锁定账户直至管理员解锁。
f) 远程登录网络设备采用 SSH 加密登录方式。
g) 网络设备的用户权限分为查看级别和配置级别。

B.1.2.8 备份及恢复

满足如下基本要求：

a) 网络配置发生改变立即备份到专用备份服务器。
b) 每周定期备份网络设备的操作系统及配置。

B.1.2.9 主机安全

主机安全主要考虑将前端应用端和后端管理端部署在虚拟服务器下的安全性。

B.1.2.10 虚拟服务器加固

满足如下基本要求：

a) 定义统一虚拟服务器加固标准。
b) 制作虚拟机服务器映像时按照加固标准进行配置加固，并打上所有可用的安全补丁。
c) 持续关注安全公告，至少每月更新一次虚拟机服务器映像，以保证虚拟机服务器映像满足最新的安全要求。
d) 所有虚拟机服务器实例安装基于主机的入侵检测软件。
e) 虚拟机服务器实例默认开启自动更新，以及时获取最新的安全补丁。
f) 虚拟机服务器实例依据不用操作系统安装杀毒软件并自动更新。

B.1.2.11 虚拟机隔离

虚拟机集群分为多个安全域，安全域之间使用访问控制列表进行端口级的访问控制。同一安全域内部，虚拟机之间通过宿主机隔离，Linux 虚拟机使用自带 iptables 进行隔离。

B.1.2.12 Hypervisor 安全

满足如下基本要求：

a) 安装宿主机时，对宿主机操作系统以及 Hypervisor 进行配置加固。
b) Hypervisor 变更是否经过 QA 验证、安全评估。
c) Hypervisor 的操作必须通过双因素认证方式登录堡垒机后进行，操作过程必须实时审计。

B.1.2.13 虚拟机管理

满足如下基本要求：

a) 采用虚拟化在线管理系统对虚拟资源进行管理。
b) 虚拟化在线管理系统支持虚拟机服务器的弹性扩容。
c) 虚拟机映像文件妥善保存并加密，防止攻击者获取映像或快照。

B.1.2.14 虚拟机的迁移

满足如下基本要求：

a) 当虚拟机实例从一台硬件服务器转移到另外一台硬件服务器时，实时对其过程进行审计、监控和告警。虚拟机实例迁移后，消除原有物理机上磁盘和内存数据，使得虚拟机实例无法恢复。
b) 存储虚拟机数据的磁盘报废、送修前，所有的存储介质均必须消磁后方能进行下一步操作，从而避免数据泄露的安全风险。

B.1.2.15 主机身份鉴别

满足如下基本要求：

a) 采用堡垒机方式登录服务器，堡垒机支持用户名＋静态密码＋动态口令的方式对用户身份标识和鉴别。
b) 设置 VPN 账号服务器对 VPN 用户接入身份标识和鉴别。
c) 各类服务器的所有账号均设置口令，口令设置参考“微型管理端”中相关要求，禁用不需要的账号。
d) 启用登录失败处理功能，设定账户锁定阈值和账户锁定时间。
e) 采用加密传输的远程桌面管理工具管理服务器。
f) 各类账号的设置均是唯一性，以便追溯到用户。

B.1.2.16 主机访问控制

满足如下基本要求：

a) 堡垒机根据每个账户需求，设定有的权限列表 key，用户根据相应的权限列表 key 对系统资源进行访问。
b) 关闭或禁用所有系统默认账户。
c) 禁止多人共用一个账户。

B.1.2.17 主机安全审计

满足如下基本要求：

a) 采用实时审计功能对用户名、时间、事件、所做操作予以记录。
b) 对触发超出权限的操作予以邮件报警并通知管理员。
c) 保证审计记录无法被删除。
d) 定期查看和备份审计记录。

B.1.2.18 主机入侵防范

操作系统遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。

B.1.2.19 主机恶意代码防范

满足如下基本要求：

a) 架设防病毒服务器，实时自动下载、更新防病毒软件及病毒定义。

b) 各类服务器统一安装病毒服务器的客户端程序，不在同一服务器上安装有两种及以上防病毒客户端程序。

c) 每台服务器开启防病毒客户端实时监控功能，定期进行计算机病毒检测，并保持防毒软件或病毒特征库的实时更新。

B.1.2.20 主机资源控制

采用第三方主机监控系统对服务器 CPU、硬盘、内存、网络等资源予以监控。

B.1.2.21 主机备份及恢复

支持实时备份，备份至少保留三个副本。

B.1.3 应用安全

B.1.3.1 安全开发

满足如下基本要求：

a) 建立安全开发流程，参与到需求分析、产品设计、开发编码、产品测试、系统发布过程中，通过软件开发的螺旋开发模式，考虑系统安全性。

b) 需求分析阶段：根据功能需求文档进行安全需求分析，针对业务内容、业务流程、技术框架进行沟通，形成《安全需求分析建议》，并与业务方、开发人员就其中建议达成共识。根据项目特征，与测试人员沟通安全测试关键点，形成《安全测试建议》。

c) 产品设计阶段：结合《安全需求分析建议》，评审产品设计文档。同时根据产品设计文档，对产品设计中采用的技术进行安全评估，形成《产品设计安全建议》，并与开发人员就安全建议达成共识。

d) 开发编码阶段：开发过程中开发需要遵守各类《安全开发规范》，避免出现不安全的代码。

e) 产品测试阶段：产品测试分为产品代码扫描、产品黑盒测试和产品手工测试三个部分。

f) 产品白盒测试：在产品代码发布后，使用代码扫描工具，对产品代码进行白盒扫描，输出《代码扫描报告》，开发人员根据报告中的风险点进行安全加固。

g) 产品黑盒测试：在产品代码提交后，使用黑盒扫描工具，对产品进行黑盒扫描，输出《安全测试报告》的黑盒工具扫描部分，开发人员根据报告中的风险点进行安全加固。

h) 产品手工测试：根据《安全测试建议》，针对产品白盒测试、黑盒测试中不能覆盖点，进行手动测试。在产品安全测试过程中出现的安全漏洞，视同产品缺陷，需要开发工程师重新编码修补，并且经过重新测试认可，最终输出《安全审核报告》。

i) 系统发布阶段：对系统发布进行严格管理，只有在经过产品测试，并且得到《安全审核报告》许可后，系统才能发布到线上环境，以防止产品携带安全漏洞在生产环境运行。

B.1.3.2 应用身份鉴别

满足如下基本要求：

a) 应用设计有专门的登录模块，并支持口令和用户名方式、安全控件。

b) 支持通过手机短信方式获取动态口令。

c) 具备身份标识唯一性检查功能。

d) 具备用户身份鉴别信息复杂度检查功能，口令长度要求 6 位，包含数字、大小写字母。

e) 不允许存在空口令账户。

f) 若登录多次未成功，设计需要输入验证码，下次登录成功后回提示之前登录信息。

B.1.4 安全保障系统

B.1.4.1 网页漏洞检测

对网站面临的 SQL 注入、xss 跨站脚本等各项高危安全漏洞进行检测。

B.1.4.2 网站挂马检测

通过静态分析技术与虚拟机沙箱检测技术相结合，对网站进行挂马检测。

B.1.4.3 防 DDoS 服务

部署专业防 DDoS 设备来抵御 SYN flood 拒绝服务攻击。

B.1.4.4 端口安全检测

定期扫描服务器当前开放的端口，降低系统被入侵的风险。

B.1.4.5 异地登录提醒

根据网站用户的登录习惯进行分析并建立模型，对异地登录提醒通过扫描访问日志实时发现异常登录行为，并以短信或邮件的方式通知用户，避免非授权登录可能造成的损害。

B.1.4.6 主机密码暴力破解防御

提供密码破解防御实时发现非法入侵。

B.1.4.7 网站后门检测

通过扫描访问 URL 实时发现网站后门，并以短信或邮件的方式通知管理员。

B.2 办公管理端信息安全建设

B.2.1 机房物理安全

满足如下基本要求：

a) 办公网机房建设在具备基本的防震、防风、防雨能力的建筑物内，建筑物需要设置避雷针、机房设置交流电源底线。
b) 机房房顶上、活动地板下不得有水管穿过。
c) 机房设置防水层防止雨水渗入，机房窗户保持关闭。
d) 机房内需要配备手动灭火器或自动气体消防设备，定期检查、维护消防器具，并保留运行记录、维护记录和报警记录。
e) 机房出入口需要设置 24 h 视频监控，机房设置门禁系统或上锁，非机房管理员进出机房需要机房管理员邮件审批并陪同。
f) 机房所有设备放置于机架上并固定，机架、设备、线缆标识资产标签，机房内线缆采用上走线，机房电源线和通信线缆隔离铺设，用于备份的磁带、硬盘等存储介质分类标识并放置于专用柜中，机房内设置无盲区 24 h 视频监控，视频监控信息保留 3 个月，视频探头、监控记录定期检查。
g) 机房采用自动空调或精密空调将机房温度控制在 23 ℃±3 ℃，湿度 40%～55%并保持空调系统 7×24 h 工作正常。

h) 机房采用静电地板、接地的方式防止静电。

i) 机房内采用具有稳压功能的 UPS,保证短期电力供应。

B.2.2 网络安全

B.2.2.1 网络安全域的划分

满足如下基本要求:

a) 按照办公管理端局域网的安全需求,可划分为互联网接入区、服务器接入区、办公终端接入区三个安全域。

b) 安全域描述(见表 B.2)。

表 B.2 办公管理端网络安全域描述

安全域	描述
互联网接入区	用于外部互联网络接入
服务器接入区	用于内网网站、内部公文流转平台、域控服务器、防病毒服务器、补丁管理服务器、VPN 接入,仅允许内部员工访问
办公终端接入区	用于内部员工终端网络接入,仅允许内部员工访问

B.2.2.2 网络结构

满足如下基本要求:

a) 对汇聚层网络设备考虑硬件冗余。

b) 互联网接入保证足够带宽以满足内网用户的需求。

c) 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,采用 VLAN 技术划分不同的子网或网段。

B.2.2.3 入侵防范

在网络出口通过设置访问控制列表和防火墙,防止外部网络攻击。

B.2.2.4 网络访问控制

各安全域采用访问控制列表技术实现源、目的地址的端口级访问控制。

B.2.2.5 安全审计

满足如下基本要求:

a) 对网络系统中的网络设备运行状况、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。

B.2.2.6 网络设备防护

包括:

a) 采用用户名加口令的方式对登录网络设备的用户进行身份鉴别。

b) 采用绑定网络设备管理员地址的方式对网络设备的登录路径予以限制。

c) 登录网络设备的用户名具有唯一性。

d) 登录网络设备的 console 配置口令,console 口令及各类远程登录口令满足长度 8 位及以上,包

含字母和数字，每三个月定期修改口令。

e) 网络设备启用登录失败处理功能，设备登录3次验证失败后自动退出；网络登录连接超时自动退出时间<5 min。

f) 远程登录网络设备采用SSH、HTTPS等加密登录方式。

B.2.2.7 备份及恢复

每周定期备份网络设备的操作系统及配置。

B.2.3 主机安全

B.2.3.1 主机身份鉴别

满足如下基本要求：

a) 设置域账号服务器对用户登录操作进行身份标识和鉴别。

b) 设置VPN账号服务器对VPN用户接入身份标识和鉴别。

c) 各类服务器的所有账号均设置口令，口令设置参考微型管理端中相关要求，禁用不需要的账号。

d) 启用登录失败处理功能，设定账户锁定阈值和账户锁定时间。

e) 采用加密传输的远程桌面管理工具管理服务器。

f) 域账号、VPN账号的设置均唯一性，以便追溯到用户。

B.2.3.2 主机访问控制

满足如下基本要求：

a) 启用访问控制功能，依据安全策略控制用户对资源的访问，除非必需，关闭默认共享目录。

b) 重新命名管理员账户。

B.2.3.3 主机安全审计

满足如下基本要求：

a) 启用主机审计功能，覆盖对账户登录事件、账户管理、目录服务访问、登录事件、对象访问、策略更改、系统事件等类型的审核记录，事件记录应包含日期、时间、类型、主体标识、客体标识和结果等信息。

b) 定期查看和备份审计记录。

B.2.3.4 主机入侵防范

操作系统遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。

B.2.3.5 主机恶意代码防范

满足如下基本要求：

a) 架设防病毒服务器，实时自动下载、更新防病毒软件及病毒定义。

b) 各类服务器统一安装病毒服务器的客户端程序，不得在同一服务器上安装有两种及以上防病毒客户端程序。

c) 每台服务器开启防病毒客户端实时监控功能，定期进行计算机病毒检测，并保持防毒软件或病毒特征库的实时更新。

B.2.3.6 主机备份及恢复

每天定时备份操作系统及数据。

B.2.4 应用安全

B.2.4.1 应用身份鉴别

满足如下基本要求：

a) 应用设计有专门的登录模块，并支持域账号单点登录。

b) 所有帐号都有唯一的 ID(身份标识)，均有域账号认证。

c) 应用系统需启用登录失败处理功能，登录多次未成功，能自动断开。

B.2.4.2 应用访问控制

满足如下基本要求：

a) 应用系统根据不同用户的角色分配相应的权限。

b) 授予不同账户为完成各自承担任务所需的最小权限。

B.2.4.3 应用安全审计

满足如下基本要求：

a) 应用系统提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。

b) 应用系统审计记录保证无法删除、修改。

c) 审计记录的内容至少包括事件日期、时间、发起者信息、类型、描述和结果等。

B.2.4.4 通信保密性

采用加密技术如 HTTPS 保证通信过程中数据的完整性。

B.2.4.5 备份与恢复

每天定时备份应用及数据。

附 录 C
（资料性附录）
中小电子商务企业自建或资源租用模式的项目开发过程安全管理案例

C.1 开发人员的安全管理

C.1.1 参加开发项目队伍人员（以下统称开发人员）在参与重要信息系统项目开发之前，应经过严格的背景审查，并签订相关的保密协议。

C.1.2 加强开发人员的职业道德教育，提高开发人员的安全防范和保密意识，对开发人员进行安全防范技术和措施等方面的培训。

C.1.3 明确开发人员在信息系统开发过程中的安全职责和对信息系统的访问权限。

C.1.4 严格加强对系统开发环境和开发场地的出入管理，进入开发现场应经过必要的安全控制措施。

C.1.5 禁止非项目组人员未经授权进入开发现场，特殊情况下进入开发现场时应获得相应的授权。

C.2 开发设备使用的安全管理

C.2.1 做好对信息系统开发环境的安全管理，信息系统的开发环境要相对独立，开发环境与运行环境进行分离。

C.2.2 开发环境中的设备明确安全责任人；遵循谁使用谁负责的原则，公共用途的设备指定安全责任人进行保管和维护。

C.2.3 信息系统的开发环境和实施场地与生产环境和实施场地隔离。

C.2.4 严格管理开发环境中的各种移动设备、个人信息处理设备，禁止未经允许的设备接入开发环境，接入开发环境的桌面设备满足对桌面系统使用规范和防病毒系统管理规范的要求。

C.3 开发文档的安全管理

C.3.1 信息系统开发过程中的资料、文档要按照技术档案管理的有关规定进行整理和归档。

C.3.2 在文档的编写、整理过程中，要明确文档标准化格式规范。对文档的修改进行记录、评估修改对文档安全的影响，并确保文档的一致性。

C.3.3 文档中与安全相关的内容要准确、完整，并明确文档的密级以及分发范围。

C.3.4 开发过程中的各种文档，只能在授权分发范围内流转，任何人不得以各种形式进行其非授权分发或外泄。

C.4 开发过程中软件和源代码的安全管理

C.4.1 除因工作需要外，禁止任何人持有、复制软件源代码，禁止任何人外借或对外复制软件源代码。

C.4.2 信息系统开发所使用的操作系统、数据库、开发工具软件等应该使用授权的软件，不使用非授权软件。

C.4.3 应对编程语言和编程工具的使用进行培训，了解和掌握编程语言和编程工具已知的安全隐患，加强对源代码的检查，防止源代码中存在可疑程序和已知的安全隐患。

C.4.4 严格控制信息系统所采用的关键技术措施和核心安全功能设计的发放范围，对于自行编制的加

密算法采用二次加密控制并由不同人员分别编程实现。对于重要的秘密资源(如源程序、目标码等)严格设置访问权限控制。

C.4.5 对应用系统的编译过程进行严格监督,确保经正确编译的软件版本最终生成运行代码,并保证运行代码的完整性、安全性。

C.4.6 严格控制对软件版本的管理,确保信息系统开发过程中源代码和执行代码的一致性和正确性。

参 考 文 献

[1] GB/T 18811 电子商务基本术语

[2] GB/T 20271 信息安全技术 信息系统通用安全技术要求

[3] GB/T 20275 信息安全技术 入侵检测系统技术要求和测试评价方法

[4] GB/T 20279 信息安全技术 网络和终端设备隔离部件安全技术要求

[5] GB/T 20281 信息安全技术 防火墙技术要求和测试评价方法

[6] GB/T 20945 信息安全技术 信息系统安全审计产品技术要求和测试评价方法

[7] GB/T 20984 信息安全技术 信息安全风险评估规范

[8] GB/T 22080 信息技术 安全技术 信息安全管理实用规则

[9] GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

[10] GB/T 22240 信息安全技术 信息系统安全等级保护定级指南

[11] GB/T 25060 信息安全技术 公钥基础设施 X.509 数字证书应用接口规范

[12] GB/T 25068 信息技术 安全技术 IT 网络安全

[13] GB/T 25069 信息安全技术 术语

[14] GB/T 28448 信息安全技术 信息系统安全等级保护测评要求

[15] GB/T 28452 信息安全技术 应用软件系统通用安全技术要求

[16] GB/T 28453 信息安全技术 信息系统安全管理评估要求

[17] GB/Z 28828 信息安全技术 公共及商用服务信息系统个人信息保护指南

[18] GB/T 29765 信息安全技术 数据备份与恢复产品技术要求与测试评价方法

[19] GB/T 29766 信息安全技术 网站数据恢复产品技术要求与测试评价方法

[20] GB/T 30279 信息安全技术 安全漏洞等级划分指南

[21] GB/T 31168 信息安全技术 云计算服务安全能力要求

[22] GA/T 708 信息安全技术 信息系统安全等级保护体系架构

[23] ISO/IEC 27000 Information technology—Security techniques—Information security management systems—Overview and vocabulary

中 华 人 民 共 和 国
国家标准化指导性技术文件
信息安全技术
中小电子商务企业信息安全建设指南
GB/Z 32906—2016
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 2.25　字数 62 千字
2016 年 9 月第一版　2016 年 9 月第一次印刷
*
书号:155066·1-55103　定价　33.00 元

GB/Z 32906-2016