急　件

中国人民银行文件

银发〔2010〕19号

中国人民银行关于印发《网上银行系统信息安全通用规范（试行）》的通知

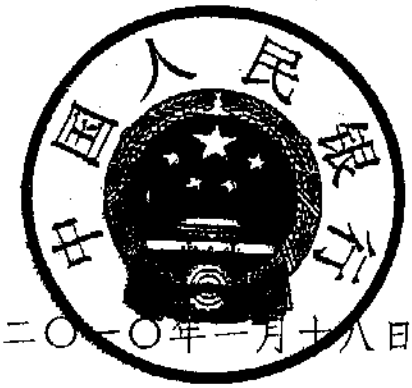
中国人民银行上海总部，各分行、营业管理部，各省会（首府）城市中心支行，副省级城市中心支行；各政策性银行、国有商业银行、股份制商业银行，中国邮政储蓄银行：

为加强网上银行管理，促进网上银行业务健康发展，有效增强网上银行系统的信息安全防范能力，中国人民银行制定了《网上银行系统信息安全通用规范（试行）》，现印发给你们，请遵照执行。

请中国人民银行上海总部，各分行、营业管理部、省会（首府）城市中心支行，副省级城市中心支行将本通知转发至辖区内各城市商业银行、农村商业银行、城市信用社和农村信用社。

执行中如遇问题，请及时告知中国人民银行科技司。

附件：网上银行系统信息安全通用规范（试行）



二〇一〇年一月十八日

主题词：金融科技　信息安全　通知

抄　　送：银监会，各直属企事业单位，中国银联股份有限公司，上海黄金交易所，汇达公司，交易商协会，上海清算所。

内部发送：各司局，党委各部门。

联系人：董贞良　　联系电话：66194640　　（共印 95 份）

中国人民银行办公厅　　2010 年 1 月 19 日印发

附件

网上银行系统信息安全通用规范

（试行）

中国人民银行

目　　录

前　言

本规范是在收集、分析评估检查发现的网上银行系统信息安全问题和已发生过的网上银行案件的基础上，有针对性提出的安全要求，内容涉及网上银行系统的技术、管理和业务运作三个方面。

本规范分为基本要求和增强要求两个层次。基本要求为最低安全要求，增强要求为本规范下发之日起的三年内应达到的安全要求，各单位应在遵照执行基本要求的同时，按照增强要求，积极采取改进措施，在规定期限内达标。

本规范旨在有效增强现有网上银行系统安全防范能力，促进网上银行规范、健康发展。本规范既可作为网上银行系统建设和改造升级的安全性依据，也可作为各单位开展安全检查和内部审计的依据。

1 使用范围和要求

本规范指出了网上银行系统的描述、安全技术规范、安全管理规范、业务运作安全规范，适用于规范网上银行系统建设、运营及测评工作。

2 规范性引用文件

下列文件中的条款通过本规范的引用而成为本规范的条款。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规范，然而，鼓励根据本规范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规范。

GB/T 20983-2008 信息安全技术 网上银行系统信息安全保障评估准则

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 20984-2007 信息安全技术 信息系统风险评估规范

GB/T 18336.1-2008 信息技术安全技术信息技术安全性评估准则第 1 部分:简介和一般模型

GB/T 18336.2-2008 信息技术安全技术信息技术安全性评估准则第 2 部分: 安全功能要求

GB/T 18336.3-2008 信息技术安全技术信息技术安全性评估准则第 3 部分: 安全保证要求

GB/T 22080-2008 信息技术 安全技术 信息安全管理体系要求

GB/T 22081-2008 信息技术 安全技术 信息安全管理使用规则

GB/T 14394-2008 计算机软件可靠性和可维护性管理

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

《中国人民银行关于进一步加强银行业金融机构信息安全保障工作的指导意见》（银发〔2006〕123 号）

《中国人民银行 中国银行业监督管理委员会 公安部 国家工商总局关于加强银行卡安全管理预防和打击银行卡犯罪的通知》（银发〔2009〕142 号）

《中国人民银行办公厅关于贯彻落实<中国人民银行 中国银行业监督管理委员会 公安部 国家工商总局关于加强银行卡安全管理预防和打击银行卡犯罪的通知>的意见》（银办发〔2009〕149号）

3 术语和定义

GB/T 20274 确立的以及下列术语和定义适用于本规范。

3.1 网上银行

商业银行等金融机构通过互联网等公众网络基础设施，向其客户提供各种金融业务。

3.2 互联网

因特网或其他类似形式的通用性公共计算机通信网络。

3.3 敏感信息

任何影响网上银行安全的密码、密钥以及交易数据等信息，密码包括但不限于转账密码、查询密码、登录密码、证书的 PIN 码等。

3.4 客户端程序

为网上银行客户提供人机交互功能的程序，以及提供必需功能的组件，包括但不限于：可执行文件、控件、静态链接库、动态链接库等。

3.5 USBKey

一种 USB 接口的硬件设备。它内置单片机或智能卡芯片，有一定的存储空间，可以存储用户的私钥以及数字证书。

3.6 USB Key 固件

影响 USB Key 安全的程序代码。

3.7 强效加密

一个通用术语，表示极难被破译的加密算法。加密的强壮性取决于所使用的加密密钥。密钥的有效长度应不低于可比较的强度建议所要求的最低密钥长度。对于基于密钥的系统（例如 3DES），应不低于 80 位。对于基于因子的公用密钥算法（例如 RSA），应不低于 1024 位。

4 符号和缩略语

以下缩略语和符号表示适用于本规范：

CA	数字证书签发和管理机构（Certification Authority）
Cookies	为辨别客户身份而储存在客户本地终端上的数据
COS	卡片操作系统（Card Operating System）
C/S	客户机/服务器 (Client/Server)
DOS/DDOS	拒绝服务/分布式拒绝服务（Denial of Service/Distributed of Service）
IDS/IPS	入侵检测系统/入侵防御系统（Intrusion Detection System/ Intrusion Prevention System）
IPSEC	IP 安全协议
OTP	一次性密码 （One Time Password）
PKI	公钥基础设施（Public Key Infrastructure）
SSL	安全套接字层（Secure Socket Layer）
SPA/DPA	简单能量分析/差分能量分析 (Simple Power Analysis/ Differential Power Analysis)
SEMA/DEMA	简单电磁分析/差分电磁分析 （Simple Electromagnetism Analysis/ Differential Electromagnetism Analysis）
TLS	传输层安全（Transfer Layer Secure）
VPN	虚拟专用网络（Virtual Private Network）

5 网上银行系统概述

5.1 系统标识

在系统标识中应标明以下内容：

－名称：XX 银行网上银行系统

－所属银行

5.2 系统定义

网上银行系统是商业银行等金融机构通过互联网等公众网络基础设施，向其客户提供各种金融业务服务的一种重要信息系统。网上银行系统将传统的银行业务同互联网等资源和技术进行融合，将传统的柜台通过互联网向客户进行延伸，是商业银行等金融机构在网络经济的环境下，开拓新业务、方便客户操作、改善服务质量、推动生产关系变革等的重要举措，提高了商业银行等金融机构的社会效益和经济效益。

5.3 系统描述

网上银行系统主要由客户端、通信网络和服务器端组成。

5.3.1 客户端

网上银行系统客户端不具备或不完全具备专用金融交易设备的可信通讯能力、可信输出能力、可信输入能力、可信存储能力和可信计算能力，因此，需要辅助安全设备，并通过接受、减轻、规避及转移的策略来应对交易风险。

因此，网上银行系统客户端应包括基本交易终端和专用辅助安全设备。

基本交易终端目前主要为电脑终端，将来可包括手机、固定电话等。

专用辅助安全设备用于保护数字证书、动态口令和静态密码等，应按照其在交易中具备的可信通讯能力、可信输出能力、可信输入能力、可信存储能力和可信计算能力五种能力的组合对其进行分类分析，并制订与之适应的交易安全风险防范策略。

5.3.2 通信网络

网上银行借助互联网技术向客户提供金融服务，其通信网络的最大特点是开放性，开放性带来的优点是交易成本的降低和交易便利性的提高，缺点是交易易受到安全威胁及通讯稳定性降低。因此，网上银行业务设计应充分利用开放网络低成本和便利的特点，有效应对开放网络通讯安全威胁，同时采取手段提高交易稳定性和成功率。

5.3.3 服务器端

网上银行系统服务器端用于提供网上银行应用服务和核心业务处理，应充分利用各种先进的物理安全技术、网络安全技术、主机安全技术、访问控制技术、密码技术、安全审计技术、系统漏洞检测技术和黑客防范技术，在攻击者和受保护的资源间建立多道严密的安全防线。

5.4 安全域

网上银行系统是一个涉及不同的应用系统、客户对象、数据敏感程度等的复杂信息系统。在网上银行系统的描述中，应根据应用系统、客户对象、数据敏感程度等划分安全域。

安全域是一个逻辑的划分，它是遵守相同的安全策略的用户和系统的集合。通过对安全域的描述和界定，就能更好地对网上银行系统信息安全保障进行描述。具体而言，网上银行系统主要包括：客户端、网上银行访问子网、网上银行业务系统、中间隔离设备和安全认证设备等。如图 1 所示：

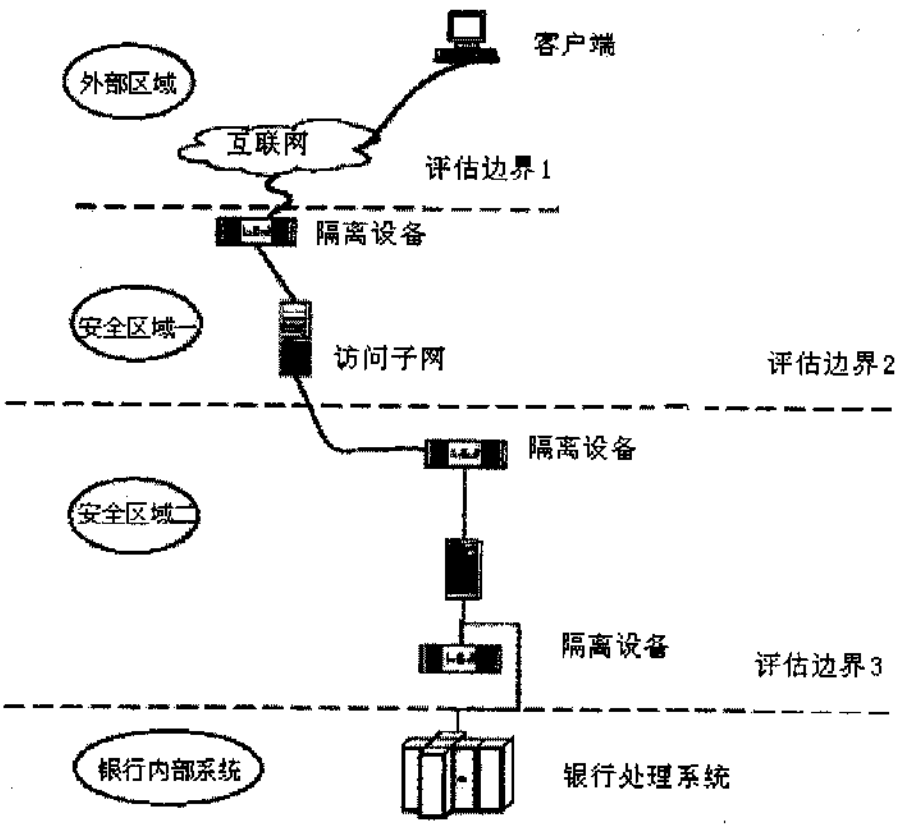


图 1 网上银行系统子安全域划分示例图

外部区域：网上银行的用户，安装网上银行客户端，通过互联网访问网上银行业务系统；

安全区域一：网上银行访问子网，主要提供客户的 Web 访问；

安全区域二：网上银行业务系统，主要进行网上银行的业务处理；

银行内部系统：银行处理系统，主要进行银行内部的数据处理。

6 安全规范

作为金融机构 IT 业务应用系统之一，网上银行系统需要与其他业务应用系统一起纳入金融机构全面的风险管理体系中。网上银行信息安全规范可分为安全技术规范、安全管理规范和业务运作安全规范。安全技术规范从客户端安全、专用辅助安全设备安全、网络通信安全和网上银行服务器端安全几个方面提出；安全管理规范从组织结构、管理制度、人员及文档管理和系统运行管理几个方面提出，业务运作安全规范从业务申请及开通、业务安全交易机制、客户教育几个方面提出。下面将分别对其进行阐述。

6.1 安全技术规范

6.1.1 客户端安全

6.1.1.1 客户端程序

A. 基本要求：

a) 客户端程序上线前应进行严格的代码安全测试，如果客户端程序是外包给第三方机构开发的，金融机构应要求开发商进行代码安全测试。金融机构应建立定期对客户端程序进行安全检测的机制。

b) 客户端程序应通过指定的第三方中立测试机构的安全检测。

c) 客户端程序应具有抗逆向分析、抗反汇编等安全性防护措施，防范攻击者对客户端程序的调试、分析和篡改。

d) 客户端程序的临时文件中不应出现敏感信息，临时文件包括但不限于 Cookies。客户端程序应禁止在身份认证结束后存储敏感信息，防止敏感信息的泄露。

e) 客户端程序应防范键盘窃听敏感信息，例如防范采用挂钩 Windows 键盘消息等方式进行键盘窃听，并应具有对通过挂钩窃听键盘信息进行预警的功能。

f) 客户端程序应防范恶意程序获取或篡改敏感信息，例如使用浏览器接口保护控件进行防范。

B. 增强要求：

a) 客户端程序应保护在客户端启动的用于访问网上银行的进程，防止非法程序获取该进程的访问权限。

b) 进行转账类交易时，客户端程序应采取防范调试跟踪的措施，例如开启新的进程。

c) 客户端程序应采用反屏幕录像技术，防止非法程序获取敏感信息。

6.1.1.2 密码保护

A. 基本要求：

a) 禁止明文显示密码，应使用相同位数的同一特殊字符（例如*和#）代替。

b) 密码应有复杂度的要求，包括：

- 长度至少 6 位，支持字母和数字共同组成。
- 在客户设置密码时，应提示客户不使用简单密码。

c) 如有初始密码，首次登录时应强制客户修改初始密码。

d) 应具有防范暴力破解静态密码的保护措施，例如在登录和交易时使用图形认证码，图形认证码应满足：

- 由数字和字母组成。
- 随机产生。
- 包含足够的噪音干扰信息，避免恶意代码自动识别图片上的信息。
- 具有使用时间限制并仅能使用一次。

e) 使用软键盘方式输入密码时，应对整体键盘布局进行随机干扰。

f) 应保证密码的加密密钥的安全。

g) 应提醒客户区分转账密码与其他密码。

B. 增强要求：

a) 采用辅助安全设备（例如 USB Key 或专用密码输入键盘）输入并保护密码。

b) 密码输入后立即加密，敏感信息在应用层保持端到端加密，即保证数据在从源点到终点的过程中始终以密文形式存在。

6.1.1.3 登录控制

A. 基本要求：

a) 设置连续失败登录次数为 10 次以下，超过限定次数应锁定网上银行登录权限。

b) 退出登录或客户端程序、浏览器页面关闭后，应立即终止会话，保证无法通过后退、直接输入访问地址等方式重新进入登录后的网上银行页面。

c) 退出登录时应提示客户取下专用辅助安全设备，例如 USB Key。

B. 增强要求：

屏蔽客户端使用 Ctrl+N 等快捷键等方式重复登录。

6.1.2 专用辅助安全设备安全

6.1.2.1 USB Key

A. 基本要求：

a) 金融机构应使用指定的第三方中立测试机构安全检测通过的 USB Key。

b) 应在安全环境下完成 USB Key 的个人化过程。

c) USB Key 应采用具有密钥生成和数字签名运算能力的智能卡芯片，保证敏感操作在 USB Key 内进行。

d) USB Key 的主文件（Master File）应受到 COS 安全机制保护，保证客户无法对其进行删除和重建。

e) 应保证私钥在生成、存储和使用等阶段的安全：

- 私钥应在 USB Key 内部生成，不得固化密钥对和用于生成密钥对的素数。
- 禁止以任何形式从 USB Key 读取或写入私钥。

- 私钥文件应与普通文件类型不同，应与密钥文件类型相同或类似。
- USB Key 在执行签名等敏感操作前应经过客户身份鉴别。
- USB Key 在执行签名等敏感操作时，应具备操作提示功能，包括但不限于声音、指示灯、屏幕显示等形式。

f) 参与密钥、PIN 码运算的随机数应在 USB Key 内生成，其随机性指标应符合国际通用标准的要求。

g) 密钥文件在启用期应封闭，禁止以添加新密钥文件的方式对密钥进行删除操作。

h) 签名交易完成后，状态机应立即复位。

i) 应保证 PIN 码和密钥的安全：

- 采用安全的方式存储和访问 PIN 码、密钥等敏感信息。
- PIN 码和密钥（除公钥外）不能以任何形式输出。
- 经客户端输入进行验证的 PIN 码在其传输到 USB Key 的过程中，应加密传输，并保证在传输过程中能够防范重放攻击。
- PIN 码连续输错次数达到错误次数上限（不超过 6 次），USB Key 应锁定。
- 同一型号 USB Key 在不同银行的网上银行系统中应用时，应使用不同的根密钥，且主控密钥、维护密钥、传输密钥等对称算法密钥应使用根密钥进行分散。

j) USB Key 使用的密码算法应经过国家主管部门认定。

k) 应设计安全机制保证 USB Key 驱动的安全，防止被篡改或替换。

l) 对 USB Key 固件进行的任何改动，都必须经过归档和审计，以保证 USB Key 中不含隐藏的非法功能和后门指令。

m) USB Key 应具备抵抗旁路攻击的能力，包括但不限于：

- 抗 SPA/DPA 攻击能力
- 抗 SEMA/DEMA 攻击能力

n) 在外部环境发生变化时，USB Key 不应泄漏敏感信息或影响安全功能。外部环境的变化包含但不限于：

- 高低温
- 高低电压

- 强光干扰
- 电磁干扰
- 紫外线干扰
- 静电干扰
- 电压毛刺干扰

B. 增强要求：

a) USB Key 应能够防远程挟持，例如具有屏幕显示、语音提示、按键确认等功能，可对交易指令完整性进行校验、对交易指令合法性进行鉴别、对关键交易数据进行输入和确认。

b) 未经按键确认，USB Key 不得签名和输出，在等待一段时间后，可自动清除数据，并复位状态。

c) USB Key 应能够自动识别待签名数据的格式，识别后在屏幕上显示签名数据或对其进行语音提示。

6.1.2.2 文件证书

此部分要求仅针对 C/S 模式客户端。

A. 基本要求：

a) 应强制使用密码保护私钥，防止私钥受到未授权的访问。

b) 用于签名的公私钥对应在客户端生成，禁止由服务器生成。私钥只允许在客户端使用和保存。

c) 私钥导出时，客户端应对客户进行身份认证，例如验证访问密码等。

d) 应支持私钥不可导出选项。

e) 私钥备份时，应提示或强制放在移动设备内，备份的私钥应加密保存。

B. 增强要求：

在备份或恢复私钥成功后，金融机构应通过第二通信渠道（例如，手机短信）向客户发送提示消息。

6.1.2.3 OTP 令牌

A. 基本要求：

a) 金融机构应使用指定的第三方中立测试机构检测通过的 OTP 令牌设备。

b) 口令生成算法应经过国家主管部门认定。

c) 动态口令的长度不应少于 6 位。

d) 应防范通过物理攻击的手段获取设备内的敏感信息，物理攻击的手段包括但不限于开盖、搭线、复制等。

e) OTP 令牌应具备抵抗旁路攻击的能力，包括但不限于：

- 抗 SPA/DPA 攻击能力
- 抗 SEMA/DEMA 攻击能力

f) 在外部环境发生变化时，OTP 令牌不应泄漏敏感信息或影响安全功能。外部环境的变化包含但不限于：

- 高低温
- 强光干扰
- 电磁干扰
- 紫外线干扰
- 静电干扰

B. 增强要求：

a) 采用基于挑战应答的动态口令，以防范中间人攻击。

b) OTP 认证系统应提供双因素认证功能。

c) OTP 令牌设备应使用 PIN 码保护等措施，确保只有授权客户才可以使用。

d) PIN 码和种子应存储在 OTP 令牌设备的安全区域内或使用其他措施对其进行保护。

e) PIN 码连续输入错误次数达到错误次数上限（不超过 6 次），OTP 令牌应锁定。

6.1.2.4 动态密码卡

基本要求：

a) 动态口令的长度不应少于 6 位。

b) 服务器端应随机产生口令位置坐标。

c) 应设定动态密码卡使用有效期，超过有效期应作废。

d) 应使用涂层覆盖等方法保护口令。

e) 动态密码卡应与客户唯一绑定。

6.1.2.5 其他专用辅助安全设备

本部分规定的是已使用的其他专用辅助安全设备，如出现新的专用辅助安全设备，可参照 6.1.2 节的要求。

a) 手机短信动态密码：

基本要求：

- 开通手机动态密码时，应使用人工参与控制的可靠手段验证客户身份并登记手机号码。更改手机号码时，应对客户的身份进行有效验证。
- 手机动态密码应随机产生，长度不应少于 6 位。
- 应设定手机动态密码的有效时间，最长不超过 10 分钟，超过有效时间应立即作废。
- 交易的关键信息应与动态密码一起发送给客户，并提示客户确认。

b) 指纹识别：

基本要求：

- 如果通过指纹鉴别客户身份，应防止指纹数据被记录和重放。
- 禁止在远程身份鉴别中采用指纹识别。近距离身份鉴别（例如，使用专用辅助安全设备对使用者的身份鉴别）可采用指纹识别。

6.1.3 网络通信安全

本部分内容指数据在网络传输过程中采用的通讯协议和安全认证方式，不包括网络基础设施方面的内容。

6.1.3.1 通讯协议

基本要求：

a) 应使用强壮的加密算法和安全协议保护客户端与服务器之间所有连接，例如，使用SSL/ TLS 和 IPSEC 协议。

b) 如果使用 SSL 协议，应使用 3.0 及以上相对高版本的协议，取消对低版本协议的支持。

c) 客户端到服务器的 SSL 加密密钥长度应不低于 128 位；用于签名的 RSA 密钥长度应不低于 1024 位，用于签名的 ECC 密钥长度应不低于 160 位。

d) 应可防止对交易报文的重放攻击。

6.1.3.2 安全认证

A. 基本要求：

a) 网上银行服务器与客户端应进行双向身份认证。

b) 整个通讯期间，经过认证的通讯线路应一直保持安全连接状态。

c) 网上银行系统应可判断客户的空闲状态，当空闲超过一定时间后，自动关闭当前连接，客户再次操作时必须重新登录。

d) 应确保客户获取的金融机构 Web 服务器的根证书真实有效，可采用的方法包括但不限于：在客户开通网上银行时分发根证书，或将根证书集成在客户端控件下载包中分发等。

B. 增强要求：

a) 网上银行系统应判断同一次登录后的所有操作必须使用同一 IP 地址和 MAC 地址，否则服务器端自动终止会话。

b) 金融机构应使用获得国家主管部门认定的具有电子认证服务许可证的 CA 证书及认证服务。

6.1.4 服务器端安全

6.1.4.1 网络架构安全

基本要求：

a) 合理部署网上银行系统的网络架构：

- 合理划分网络区域，并将网上银行网络与办公网及其他网络进行隔离。
- 维护与当前运行情况相符的网络拓扑图，并区分可信区域与不可信区域。
- 采用 IP 伪装技术隐藏内部 IP，防止内部网络被非法访问。
- 部署入侵检测系统/入侵防御系统（IDS/IPS），对网络异常流量进行监控。
- 在所有互联网入口以及隔离区（DMZ）与内部网络之间部署防火墙，对非业务必需的网络数据进行过滤。
- 采取措施保障关键服务器时间同步，例如，设置网络时间协议（NTP）服务器。
- 互联网接入应采用不同电信运营商线路，相互备份且互不影响。
- 核心层、汇聚层的设备和重要的接入层设备均应双机热备，例如，核心交换机、服务器群接入交换机、重要业务管理终端接入交换机、核心路由器、防火墙、均衡负载器、带宽管理器及其他相关重要设备。
- 保证网络带宽和网络设备的业务处理能力具备冗余空间，满足业务高峰期和业务发展需要。

b) 访问控制：

- 在网络结构上实现网间的访问控制，采取技术手段控制网络访问权限。
- 应对重要主机的 IP 地址与 MAC 地址进行绑定。
- 禁止将管理终端主机直接接入核心交换机、汇聚层交换机、服务器群交换机、网间互联边界接入交换机和其他专用交换机。
- 明确业务必需的服务和端口，不应开放多余的服务和端口。
- 禁止开放远程拨号访问。

c) 网络设备的管理规范和安全策略：

- 将关键或敏感的网络设备存放在安全区域，应使用相应的安全防护设备和准入控制手段以及有明确标志的安全隔离带进行保护。
- 应更改网络安全设备的初始密码和默认设置。
- 在业务终端与服务器之间通过路由控制建立安全的访问路径。
- 指定专人负责防火墙、路由器和 IDS/IPS 的配置与管理，按季定期审核配置规则。
- 所有设备的安全配置都必须经过审批。
- 在变更防火墙、路由器和 IDS/IPS 配置规则之前，确保更改已进行验证和审批。

d) 安全审计和日志：

- 应对网络设备的运行状况、网络流量、管理员行为等信息进行日志记录，日志至少保存3个月。
- 审计记录应包括但不限于：事件发生的时间、相关操作人员、事件类型、事件是否成功及其他与审计相关的信息。
- 应根据记录进行安全分析，并生成审计报表。
- 应对审计记录进行保护，避免被未授权删除、修改或者覆盖。

e) 入侵防范：

- 应严格限制下载和使用免费软件或共享软件，应确保服务器系统安装的软件来源可靠，且在使用前进行测试。
- 所有外部存储设备（软盘、移动硬盘、U盘等）在使用前应进行病毒扫描。
- 制订合理的IDS/IPS的安全配置策略，并指定专人定期进行安全事件分析和安全策略配置优化。
- 应在网络边界处监视并记录以下攻击行为：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。
- 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标和攻击时间，在发生严重入侵事件时应提供报警或自动采取防御措施。

基本型网络防护架构参考图和增强型网络防护架构参考图分别见附1和附2。

6.1.4.2 系统设计安全

A. 基本要求：

a) 敏感客户参数修改（包括但不限于密码、转账限额、地址以及电话联系方式）应在一次登录过程中进行二次认证（包括但不限于静态密码+动态密码）。

b) 网上银行系统应具有保存和显示客户历史登录信息（例如时间、IP地址、MAC地址等）的功能，支持客户查询登录（包括成功登录和失败登录）、交易等历史操作。

c) 网上银行系统应根据业务必需的原则向客户端提供数据，禁止提供不必要的数据。

d) 在显示经认证成功后的客户身份证件信息时，应屏蔽部分关键内容。

e) 网上银行系统应具有详细的交易流水查询功能，包括但不限于日期、时间、交易卡号、交易金额和资金余额等信息。

f) 网上银行系统应具有账户信息变动提醒功能，可使用手机短信、电子邮件等方式实时告知客户其账户的资金变化、密码修改等重要信息。

g) 网上银行系统应具有防网络钓鱼的功能，例如显示客户预留信息等。

B. 增强要求：

a) 网上银行系统应具有设置交易限额的功能并且具有默认的金额上限。

b) 网上银行系统应支持批量银行账号查询功能和线索排查功能。

6.1.4.3 Web 应用安全

A. 基本要求：

a) 资源控制：

- 应能够对系统的最大并发会话连接数进行限制。
- 应能够对单个用户的多重并发会话进行限制。
- 应能够对一个时间段内可能的并发会话连接数进行限制。
- 当应用系统通信双方中的一方在指定时间内未作任何响应，另一方应能够自动结束会话。

b) 编码规范约束：

- 应依据安全规范编写代码，例如，在应用系统开发中，不能在程序中写入固定密钥。
- 在应用系统上线前，应对程序代码进行代码复审，识别可能的后门程序、恶意代码和安全漏洞，例如，缓冲区溢出漏洞。

c) 会话安全：

- 会话标识应随机并且唯一。
- 会话过程中应维持认证状态，防止客户通过直接输入登录后的地址访问登录后的页面。
- 转账交易后，应确保使用浏览器的“后退”功能无法查看上一交易页面的重要客户信息。

- 网上银行系统 Web 服务器应用程序应设置客户登录网上银行后的空闲时间，当超过指定时间，应自动终止会话。

d) 源代码管理：

- 源代码应备份在只读介质中（例如光盘）。
- 应严格控制对生产版本源代码的访问。
- 应对生产库源代码版本进行控制，保证当前系统始终为最新的稳定版本。

e) 防止敏感信息泄漏：

- 在网上银行系统上线前，应删除 Web 目录下所有测试脚本、程序。
- 如果在生产服务器上保留部分与 Web 应用程序无关的文件，应为其创建单独的目录，使其与 Web 应用程序隔离，并对此目录进行严格的访问控制。
- 禁止在 Web 应用程序错误提示中包含详细信息，不向客户显示调试信息。
- 禁止在 Web 应用服务器端保存客户敏感信息。
- 应对网上银行系统 Web 服务器设置严格的目录访问权限，防止未授权访问。
- 统一目录访问的出错提示信息，例如，对于不存在的目录或禁止访问的目录均以“目录不存在”提示客户。
- 禁止目录列表浏览，防止网上银行站点重要数据被未授权下载。

f) 防止 SQL 注入攻击：

- 网上银行系统 Web 服务器应用程序应对客户提交的所有表单、参数进行有效的合法性判断和非法字符过滤，防止攻击者恶意构造 SQL 语句实施注入攻击。
- 禁止仅在客户端以脚本形式对客户的输入进行合法性判断和参数字符过滤。
- 数据库应尽量使用存储过程或参数化查询，并严格定义数据库用户的角色和权限。

g) 防止跨站脚本攻击：

- 应通过严格限制客户端可提交的数据类型以及对提交的数据进行有效性检查等有效措施防止跨站脚本注入。

h) 防止拒绝服务攻击：

应防范对网上银行服务器端的 DOS/DDOS 攻击。可参考的加固措施包括但不限于：

- 与电信运营商签署 DOS/DDOS 防护协议。

- 防火墙只开启业务必需的端口并开启 DOS/DDOS 防护功能。
- 使用 DOS/DDOS 防护设备。
- 使用 IDS/IPS 设备监控并阻断恶意流量。
- 使用负载均衡设备。

6.1.4.4 数据安全

A. 基本要求：

a) 身份鉴别：

- 应对登录操作系统和数据库的用户进行身份标识和鉴别，严禁匿名登录。
- 应用系统应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。
- 为不同的操作系统和数据库访问用户分配不同的账号并设置不同的初始密码，禁止共享账号和密码。
- 首次登录应用系统或操作系统时应强制修改密码，定期更改密码。
- 应要求用户的密码长度最低为 6 位，密码必须包含字母和数字并且最长有效期为 6 个月。
- 应确保对密码进行强效加密保护，不允许明文密码出现。
- 在收到用户重置密码的请求后，应先对用户身份进行核实再进行后续操作。
- 对服务器进行远程管理时，应采取加密通信方式，防止认证信息在网络传输过程中被窃听。

b) 访问控制：

- 根据“业务必需”原则授予不同用户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。
- 明确系统中各类用户的级别及权限，操作系统和数据库特权用户应进行权限分离。
- 严格限制默认用户的访问权限，重命名系统默认用户，修改默认用户密码，及时删除多余的、过期的用户。
- 严格控制操作系统重要目录及文件的访问权限。

c) 安全审计：

- 审计范围应覆盖到服务器和管理终端上的每个操作系统用户和数据库用户。
- 审计内容应包括重要用户行为、系统资源的异常使用和重要信息系统命令的使用等系统内重要的安全相关事件。
- 审计记录包括时间、类型、访问者标识、访问对象标识和事件结果。
- 应根据记录数据进行安全分析，并生成审计报表。
- 应保护审计记录，避免遭受未授权的删除、修改或覆盖。

d) 日志管理：

- 日志系统应记录系统管理员登录的时间、登录系统的方式、失败的访问尝试、系统管理员的操作以及其他涉及数据安全的访问记录。
- 严格控制系统日志的访问权限，只有工作需要并通过审批的岗位人员才能查看系统日志。
- 定期检查日志，对其中可疑的记录进行分析审核。
- 配置专门的日志服务器，及时将日志备份到日志服务器或安全介质内。

e) 灾难备份和恢复：

- 应建立重要数据的定期数据备份机制，至少每天进行一次完整的数据增量备份，并将备份介质存放在安全区域内。
- 应对关键数据进行同城和异地的实时备份，保证业务应用能够实现实时切换。
- 应制订灾难恢复计划并定期进行测试，确保各个恢复程序的正确性和计划整体的有效性。

B. 增强要求：

a) 采用监控软件保证日志的一致性与完整性。

b) 保护审计进程，避免其遭受未预期的中断。

6.2 安全管理规范

6.2.1 组织机构

基本要求：

a) 金融机构应设置独立的网上银行系统研发、测试、集成、运行维护、管理等部门或

团队。

b) 金融机构应制订明确的网上银行部门章程并详细定义各部门人员配置。

c) 金融机构应建立风险管理架构，相关人员应详细了解本单位网上银行研发、运行及管理机构职责设置。

6.2.2 管理制度

基本要求：

a) 金融机构应建立安全管理制度体系，明确工作职责、规范工作流程、降低安全风险：

- 应制订网上银行安全管理工作的总体方针和策略。
- 应建立贯穿网上银行系统设计、编码、测试、集成、运行维护以及评估、应急处置等过程，并涵盖安全制度、安全规范、安全操作规程和操作记录手册等方面的信息安全管理制度体系。

b) 金融机构应指定或授权专门的部门或人员负责安全管理制度的制订。

c) 金融机构应定期组织相关部门和人员对安全管理制度体系的合理性和适用性进行审计，及时针对安全管理制度的不足进行修订。

6.2.3 安全策略

A. 基本要求：

a) 金融机构应制订明确的网上银行系统总体安全保障目标。

b) 金融机构应制订针对网上银行系统设计与开发、测试与验收、运行与维护、备份与恢复、应急事件处置以及客户信息保密等的安全策略。

c) 金融机构应制订网上银行系统使用的网络设备、安全设备的配置和使用的安全策略。

d) 金融机构应维护详细的资产清单，资产清单应包括资产的价值、所有人、管理员、使用者和安全等级等条目，并根据安全等级制订相应的安全保护措施。

e) 金融机构应明确系统存在的威胁，并根据威胁分析系统的脆弱性，对于已发现的风险应尽快修补或制订规避措施。

f) 金融机构应针对不同的风险规定相应的可能性等级列表，并根据风险严重等级制订

应急恢复方案和演练计划。

B. 增强要求：

a) 金融机构应规定所有数据的安全级别，并制订与其安全级别相应的保护措施。

b) 金融机构应加强风险预警能力，对短时间内单个账户在异地多笔交易等异常情况进行监控。

6.2.4 人员及文档管理

基本要求：

a) 金融机构应设置信息安全管理岗位，明确本单位各相关岗位在信息安全管理过程中所承担的责任。

b) 金融机构应与员工签署保密协议，或在劳动合同中设置保密条款。

c) 金融机构应加强关键岗位员工的安全培训，确保员工了解各自岗位职责以及违反安全规定可能导致的后果。

d) 金融机构应具有员工岗位调动或离职的安全管理制度，避免账号、设备、技术资料及相关敏感信息等泄露。

e) 金融机构应建立外来人员管理制度，提交操作记录，必要时要求其签订保密协议。

f) 金融机构应建立文档管理制度，文档资料按密级或敏感程度进行登记、分类并由专人保管，重要文档资料的使用、外借或销毁应经过审批流程并进行记录。

6.2.5 系统运行管理

6.2.5.1 网络安全管理

基本要求：

a) 金融机构应建立网络安全管理制度，并对网络安全配置、日志保存时间、安全策略、系统升级、补丁更新等方面作出规定。

b) 金融机构应实现设备的最小服务配置，并定期离线备份配置文件。

c) 所有与外部系统的连接应经过授权。

d) 金融机构应根据安全策略允许或者拒绝便携式和移动式设备的网络接入。

e) 金融机构应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

f) 金融机构应定期对系统进行漏洞扫描，及时修补发现的系统安全漏洞。

g) 金融机构应根据厂家提供的升级版本软件对网络设备进行更新，并在更新前对现有的重要文件进行备份。

6.2.5.2 密钥管理

基本要求：

a) 金融机构应制订与网上银行相关的密钥管理制度，并严格实施。

b) 敏感信息在传输前应先进行强效加密，然后通过 VPN 等加密信道在网络中传输。

c) 密钥和密码应加密存储。

d) 金融机构采用的密码算法应经过国家主管部门认定。

e) 对于所有用于加密客户数据的密钥，金融机构应制订并实施全面的密钥管理流程，包括：密钥生成、密钥分发、密钥存储、密钥更换、密钥销毁、知识分割以及双重控制密钥、防止未授权的密钥更换、更换已被知晓或可能被泄漏的密钥、收回过期或失效的密钥等。

6.2.5.3 业务连续性管理

a) 业务运行连续性：

基本要求：

- 金融机构应定期评估网上银行所面临的风险、风险发生的概率及影响。
- 金融机构应制订网上银行业务连续性策略。
- 金融机构应将网上银行业务持续性管理整合到组织的流程和结构中，明确指定相关部门负责业务持续性的管理。
- 金融机构应制订员工在应急处理和安全方面的培训计划和考核标准。
- 金融机构应定期测试并更新业务连续性计划与过程。

b) 备份与恢复：

基本要求：

- 金融机构应明确需要定期备份的重要业务数据、系统数据等。
- 金融机构应建立与备份、恢复相关的安全管理制度，对数据的备份方式、备份周期、存储介质和保存期限等方面进行规范。
- 金融机构应根据数据的重要性和数据对系统运行的影响，制订数据的备份和恢复策略，备份策略需指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输的方式等。
- 金融机构应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存。
- 金融机构应定期执行恢复程序，检查并测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

c) 应急管理：

基本要求：

- 金融机构应在网上银行统一的应急预案框架下，制订针对不同事件的应急预案，应急预案至少包括各类事件场景下启动应急预案的条件、应急处理流程、系统恢复流程、事后经验总结和培训等内容。
- 金融机构应对网上银行系统相关人员进行应急预案培训，应急预案的培训应至少每年举办一次。
- 金融机构应制订应急预案演练计划，定期对网上银行系统应急预案进行演练，每年至少开展一次实战演练。
- 应急预案应定期审查并根据实际情况及时更新。

6.3 业务运作安全规范

6.3.1 业务申请及开通

A. 基本要求：

a) 网上银行转账功能的开通必须由客户本人到柜台申请。申请时，金融机构应对其进行风险提示，验证客户的有效身份，并要求客户书面确认。客户通过已采取电子签名

验证的网上银行渠道申请转账类业务的，视同客户本人主动申请并书面确认。以下转账类业务可不受上述限制：开通同一客户账户之间转账并且金融机构能有效识别转入、转出方为同一客户账户的；客户预先通过柜台签约对转入账户进行绑定同时指定交易电话的。

b) 企业网上银行开通必须到柜台申请，申请时，金融机构应审查其申请材料的真实性、完整性和合规性。

c) 客户申请 USB Key 作为数字证书载体时，应持有效身份证件到柜台办理，金融机构应将 USB Key 设备序列号与客户进行绑定，并在客户下载证书时将其作为客户身份认证因素之一；如果 USB Key 丢失，应由客户本人持有效证件到柜台重新办理，原有数字证书作废。

d) 如果网上银行登录密码以密码信封方式发送给客户或者登录密码被设置为统一初始密码，金融机构应强制客户首次登录时修改初始密码。

6.3.2 业务安全交易机制

6.3.2.1 身份认证

基本要求：

a) 网上银行转账类操作应使用双因素身份认证。双因素身份认证由以下两种身份认证方式组成：一是客户知晓、注册的客户名称及密码；二是客户持有、特有并用于实现身份认证的信息，包括但不限于物理介质或电子设备等。以下转账类业务可不受上述限制：同一客户账户之间转账并且金融机构能有效识别转入、转出方为同一客户账户的。

b) 禁止仅使用文件证书或使用文件证书加静态密码的方式进行转账类操作。

c) 使用企业网上银行进行转账类操作时，应至少使用硬件承载的数字证书进行签名等安全认证方式。

d) 客户登录网上银行时或登录后执行账户资金操作时，若身份认证连续失败超过一定次数（不超过 10 次），应在短时间内锁定该客户网上银行登录权限，并立即通过短信或电话等方式通知客户。

e) 申请客户数字证书时，应验证公钥的有效性，证书签名请求在进入 SSL 通道前应采取安全保护措施。

f) 客户数字证书只能被下载一次。下载证书时，应有身份认证的过程，例如提交授权码和参考码。身份认证信息应设置有效期，超出有效期而未下载证书，应重新办理。

6.3.2.2 交易流程

A. 基本要求：

a) 网上银行系统应能够对客户端提交的交易进行唯一性认证，应能识别并拒绝重复交易。

b) 转账类交易中，如果客户端对交易数据签名，签名数据除流水号、交易金额、转入账号、交易日期和时间等要素外，还应包含由服务器生成的随机数据。对于从网上银行客户端提交的交易数据，服务器应验证签名的有效性并安全存储签名。

c) 转账类交易中，网上银行系统应具有防范客户端数据被篡改的机制，应由客户确认转账交易关键数据（至少包含转出账号、转入账号、交易金额、交易日期和时间），并采取有效确认方式以保证待确认的信息不被篡改，例如，由服务器以图片的形式返回待客户确认的信息或者在 USB Key 内完成确认。

d) 转账类交易中，网上银行系统应对客户端提交的敏感信息间的隶属关系进行严格校验，例如，验证提交的账号和卡号间的隶属关系以及账号、卡号与登录用户之间的关系。

e) 对于转账类交易，金融机构应充分提示客户相关的安全风险并提供及时通知客户资金变化的服务，如果客户选择该服务，应在交易发生后实时告知客户其资金变化情况。

f) 对于大额转账等高风险操作（金融机构可根据自身情况对高风险操作进行界定）发生后，金融机构应在确保客户有效联系方式前提下，立即将资金变动情况通知客户。

B. 增强要求：

转账类交易应使用第二通信渠道请求客户反馈确认交易信息，例如，使用手机短信或电话等方式。

6.3.2.3 网上支付

如果金融机构的网上银行系统与网上支付系统集成在一起，应保证不会影响彼此的安全性，并满足以下安全要求：

A. 基本要求：

a) 金融机构应根据“业务必需”原则与商户共享数据，严禁与商户共享客户的敏感信息。

b) 如果商户系统参与敏感信息的处理，金融机构应提示商户禁止存储客户的敏感信息。

c) 网上银行系统在与商户系统建立连接之前应认证商户系统的身份。

d) 网上银行系统与商户系统之间交互的数据应加密传输，加密的强度至少满足：3DES的加密密钥长度不小于128位，RSA密钥长度不小于1024位，ECC密钥长度不小于160位。

B. 增强要求：

a) 对于证券、基金及电子客票等实时性和准确性要求比较高的网上支付应用，应综合采用技术和业务手段，提高交易成功率和稳定性。

b) 商户应将客户详细账单信息传送至网上银行系统，在网上银行系统支付页面中显示供客户确认。

6.3.3 客户教育

基本要求：

a) 金融机构应通过各种宣传渠道向大众提供正确的网上银行官方网址和呼叫中心号码。

b) 金融机构应向客户印发通俗、易懂的网上银行信息安全宣传手册。

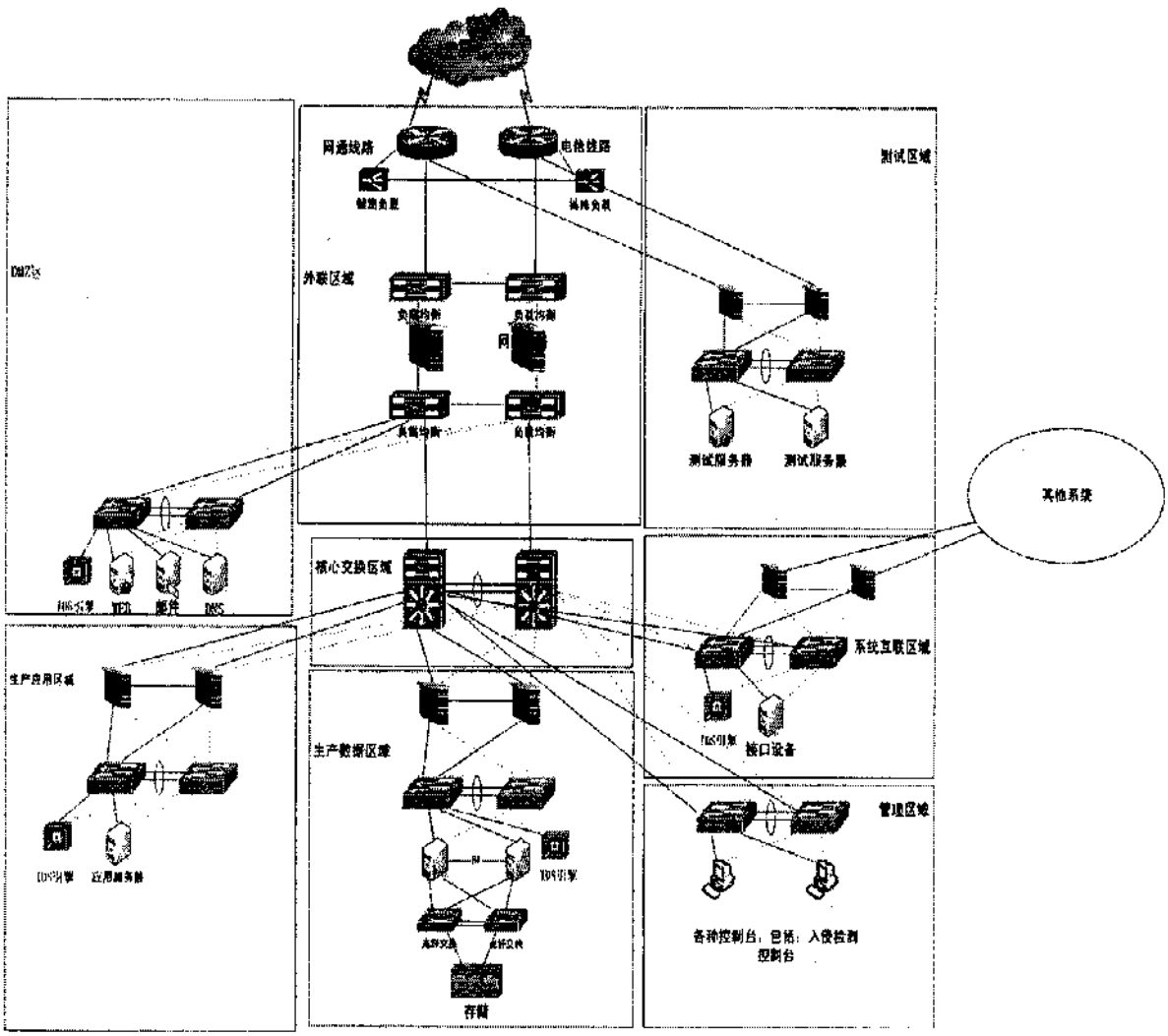
c) 在网上银行使用过程中，金融机构应向客户明确提示相关的安全风险和注意事项。

d) 金融机构应在网上银行官方网站首页显著位置开设信息安全教育栏目，包括但不限于维护良好的客户端环境、谨防虚假网上银行链接、注意对网上银行的敏感信息进行保护等内容。

附 1 基本的网络防护架构参考图

以下给出一个基本的网络安全防护架构参考图，其中：

1. 外联区：主要处理外部访问的区域。
2. DMZ 区：是一个公布信息的区域，通过互联网接入的外部客户可以访问该区域。
3. 生产应用区：是网络应用程序所处区域，处理各种逻辑业务。
4. 生产数据区：主要处理各种数据操作，是数据库所在区域。
5. 管理区域：主要负责管理设备的接入。
6. 测试区域：单独的互联网测试环境区域。
7. 系统互联区域：主要处理互联网应用系统与其他系统互联的区域。



附 2 增强的网络防护架构参考图

增强的网络安全防护是在基本安全防护的基础上，部署应用防火墙和文件摘要保护来进一步保障网络的安全性，同时通过协议分析和流量统计、操作审计、数据审计和监控审计系统来完善审计等安全需求，以下给出增强的网络安全防护架构参考图。