

中华人民共和国国家标准

GB/T 37002—2026

代替 GB/T 37002—2018

网络安全技术 电子邮件系统安全 技术规范

Cybersecurity technology—Security technology specifications for electronic
mail system

2026-07-02 发布

2027-02-01 实施

国家市场监督管理总局 发布
国家标准化管理委员会

目 次

前言 III

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 概述 3

 5.1 安全技术框架 3

 5.2 安全目标 4

 5.3 安全级别 4

6 基本级安全要求 4

 6.1 安全技术要求 4

 6.2 安全管理要求 8

 6.3 安全运行要求 10

7 增强级安全要求 13

 7.1 安全技术要求 13

 7.2 安全管理要求 15

 7.3 安全运行要求 16

8 安全要求测试评价方法 17

 8.1 安全技术要求测试评价方法 17

 8.2 安全管理要求测试评价方法 28

 8.3 安全运行要求测试评价方法 35

附录 A（资料性） 电子邮件系统安全级别选择方法 44

附录 B（资料性） 基于加密技术的电子邮件系统模型 45

参考文献 46

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 37002—2018《信息安全技术 电子邮件系统安全技术要求》，与 GB/T 37002—2018 相比，除结构调整和编辑性改动外，主要技术变化如下：

- 删除了术语“应用服务隔离机制”(见 2018 年版的 3.3)；
- 增加了“邮件应用系统”“垃圾邮件”的术语和定义(见 3.3、3.4)；
- 更改了电子邮件系统安全技术架构中安全技术要求和安全运行要求(见第 5 章图 1, 2018 年版的第 5 章图 1)；
- 更改了硬件、操作系统、支撑系统以及云计算环境等相关安全技术要求为参照相应国家标准(见 6.1.1.1、6.1.1.2、6.1.1.3、6.1.1.4, 2018 年版的 6.1.1.1、6.1.1.2、6.1.1.3、6.1.1.4)；
- 更改了身份鉴别的安全要求(见 6.1.1.5.1、7.1.1.5.1, 2018 年版的 6.1.1.5.1、7.1.1.5.1)；
- 更改了访问控制为权限管理(见 6.1.1.5.2、7.1.1.5.2, 2018 年版的 6.1.1.5.2、7.1.1.5.2)；
- 更改了用户审计的安全要求(见 6.1.1.5.3、7.1.1.5.3, 2018 年版的 6.1.1.5.3、7.1.1.5.3)；
- 更改了收发过程保护的安全要求(见 6.1.1.5.5, 2018 年版的 6.1.1.5.5)；
- 更改了邮件客户端的安全要求(见 6.1.2, 2018 年版的 6.1.2)；
- 更改了安全传输的安全要求(见 6.1.3.3、7.1.3.3, 2018 年版的 6.1.3.3、7.1.3.3)；
- 增加了云计算环境相关安全管理与运行要求(见 6.2.7、6.3.3、6.3.9、6.3.10)；
- 更改了网络安全监测的安全要求(见 6.3.3, 2018 年版的 6.3.3)；
- 更改了反垃圾邮件、防病毒的安全要求(见 6.3.4、6.3.5, 2018 年版的 6.3.4、6.3.5)；
- 增加了防钓鱼的安全要求(见 6.3.6)；
- 增加了基础设施的安全要求(见 6.3.10)；
- 增加了管理员操作终端访问控制要求(见 7.2.5)；
- 增加了安全要求测试评价方法(见第 8 章)。

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专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：国家信息技术安全研究中心、中国电子技术标准化研究院、深圳奥联信息安全技术有限公司、中移动信息技术有限公司、国家信息中心、中国信息安全测评中心、北京国信安邮科技有限公司、国家计算机网络应急技术处理协调中心、国家计算机网络应急技术处理协调中心北京分中心、中资网络信息安全科技有限公司、北京安宁创新网络科技股份有限公司、广东盈世计算机科技有限公司、北京亿中邮信息技术有限公司、公安部第一研究所、上海市信息安全测评认证中心、西安邮电大学、中科信息安全共性技术国家工程研究中心有限公司、北京时代亿信科技股份有限公司、公安部第三研究所、北京神州绿盟科技有限公司、北京网际思安科技有限公司、中国电子科技集团公司第十五研究所、天翼安全科技有限公司、中国核能电力股份有限公司、南方电网数字电网集团信息通信科技有限公司、启明星辰信息技术集团股份有限公司、远江盛邦安全科技集团股份有限公司、上海斗象信息科技有限公司、长扬科技(北京)股份有限公司、天翼云科技有限公司、用友网络科技股份有限公司、中电信量子信息科技集团有限公司、奇安信网神信息技术(北京)股份有限公司、三未信安科技股份有限公司、昆仑数智科技有限责任公司、中科方德软件有限公司、国网吉林省电力有限公司。

本文件主要起草人：姚佳明、李京春、刘红庆、张卫博、王惠莅、程朝辉、王阳、罗海宁、任飞、欧阳文蕾、

刘楠、杨梦竹、蔡先勇、但波、饶华一、陈旭、杨韬、陈晨、吴冬宇、刘鸿运、郑瑞刚、李文杰、潘进、陈牧谦、李一鸣、蔡磊、高强、林延中、张中华、李海威、徐佟海、张勇、伊鹏达、李继国、宋好好、陈爱珍、汪楫人、孙琪、梁伟、梁浩、张佳发、吴杨、郝龙、徐钟豪、赵华、辛晨、季晟宇、刘勇、安锦程、张玉涛、高辰、王少航、祝英杰。

本文件及其所代替文件的历次版本发布情况为：

——2018 年首次发布为 GB/T 37002—2018；

——本次为第一次修订。

网络安全技术 电子邮件系统安全技术规范

1 范围

本文件规定了电子邮件系统网络安全要求,包括电子邮件系统的安全技术要求、安全管理要求、安全运行要求,并描述了测试评价方法。

本文件适用于电子邮件系统的设计、建设、使用和测试评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 20272—2026 网络安全技术 操作系统安全技术规范
GB/T 20273—2019 信息安全技术 数据库管理系统安全技术要求
GB/T 25069—2022 信息安全技术 术语
GB/T 26232—2025 信息技术 中间件 应用服务器中间件技术要求
GB/T 30282—2023 信息安全技术 反垃圾邮件产品技术规范
GB/T 31167—2023 信息安全技术 云计算服务安全指南
GB/T 31168—2023 信息安全技术 云计算服务安全能力要求
GB/T 32915—2026 网络安全技术 二元序列随机性检测方法
GB/T 39680—2020 信息安全技术 服务器安全技术要求和测评准则
GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
GB/T 43698—2024 网络安全技术 软件供应链安全要求
GB/T 44886.4—2026 网络安全技术 网络安全产品互联互通 第4部分:威胁信息格式
GM/T 0018—2023 密码设备应用接口规范
GM/T 0021—2023 动态口令密码应用技术规范
GM/T 0028—2024 密码模块安全要求

3 术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

电子邮件系统 electronic mail system

支撑用户使用电子邮件服务的信息系统。

注1: 电子邮件系统由电子邮件客户端、电子邮件服务器、外围安全防护设备三部分组成。

注2: 本文件中电子邮件系统简称为邮件系统。

3.2

电子邮件服务器 **electronic mail server**

为客户端提供邮件应用服务的计算机系统,由服务器硬件、操作系统、支撑系统(中间件和数据库)和电子邮件应用系统组成。

注:本文件中电子邮件服务器简称为邮件服务器。

3.3

电子邮件应用系统 **electronic mail application system**

电子邮件服务器中对电子邮件业务进行处理的软件系统集合。

注:本文件中电子邮件应用系统简称为邮件应用系统。

3.4

垃圾邮件 **spam**

用户事先未提出请求或不同意接收的电子邮件。

注:垃圾邮件一般具有如下特征:

- 含有用户不愿意接收的广告、宣传材料等内容;
- 同时发送给大量用户;
- 含有虚假的信息源、发件人、路由等信息;
- 含有恶意代码。

[来源:GB/T 30282—2023,3.1]

3.5

用户身份数字凭证 **user digital certificates**

用户通过身份鉴别后,由鉴别者为用户出具的一种可信的身份电子凭据。

3.6

“挑战-应答”认证方式 **“challenge-response” authentication method**

一类基于零知识证明的身份鉴别协议。

注:在每次认证过程中,由认证方提出不同的挑战问题,被认证方做出应答,认证方通过验证应答的正确性,进而确认被认证方的身份。

3.7

邮件传输协议 **mail transfer protocol**

在网络环境中传输电子邮件的协议标准。

示例:邮件发送协议(SMTP)、邮件收取协议(POP3/IMAP)。

3.8

数据加密设备 **data encryption device**

独立或并行为多个应用实体提供密码服务和密钥管理的设备。

3.9

内容加密密钥 **content encryption key**

用于加密数据内容的临时密钥。

3.10

中间件 **middle ware**

连接 Web 服务和电子邮件应用系统的计算机软件。

注:电子邮件应用系统在中间件的支撑下提供 Web 方式的邮件收发和后台管理服务。

3.11

网盘 **online disk**

电子邮件系统提供的网络文件存储功能,一般用于邮件附件的在线存储与分享。

4 缩略语

下列缩略语适用于本文件。

B/S:浏览器/服务器结构(browser/server)

C/S:客户端/服务器结构(client/server)

CTID:居民身份网络可信凭证(cyber trusted identity)

DKIM:域密钥识别邮件(domainKeys identified mail)

ID:标识符(identifier)

IMAP:交互邮件访问协议(Internet mail access protocol)

IP:互联网协议/网间协议(Internet protocol)

MAC:消息鉴别码(message authentication code)

POP3:邮局协议的第3个版本(post office protocol 3)

SDK:软件开发工具包(software development kit)

SMTP:简单邮件传输协议(simple mail transfer protocol)

SPF:发件人策略框架(sender policy framework)

SQL:结构化查询语言(structured query language)

SSL:安全套接字协议(secure sockets layer)

TLS:传输层安全协议(transport layer security protocol)

URL:统一资源定位符(uniform resource locator)

Web:万维网(world wide web)

5 概述

5.1 安全技术框架

电子邮件系统安全技术框架由安全技术、安全管理、安全运行三部分组成,安全技术框架如图1所示。安全技术包括邮件服务器、邮件客户端、邮件数据的安全。安全管理包括电子邮件系统管理所涉及的诸如用户管理、密钥管理、配置管理和数据库管理等。安全运行包括电子邮件系统运行所涉及的诸如边界保护、网络安全监测、防病毒、反垃圾邮件和安全审计等。

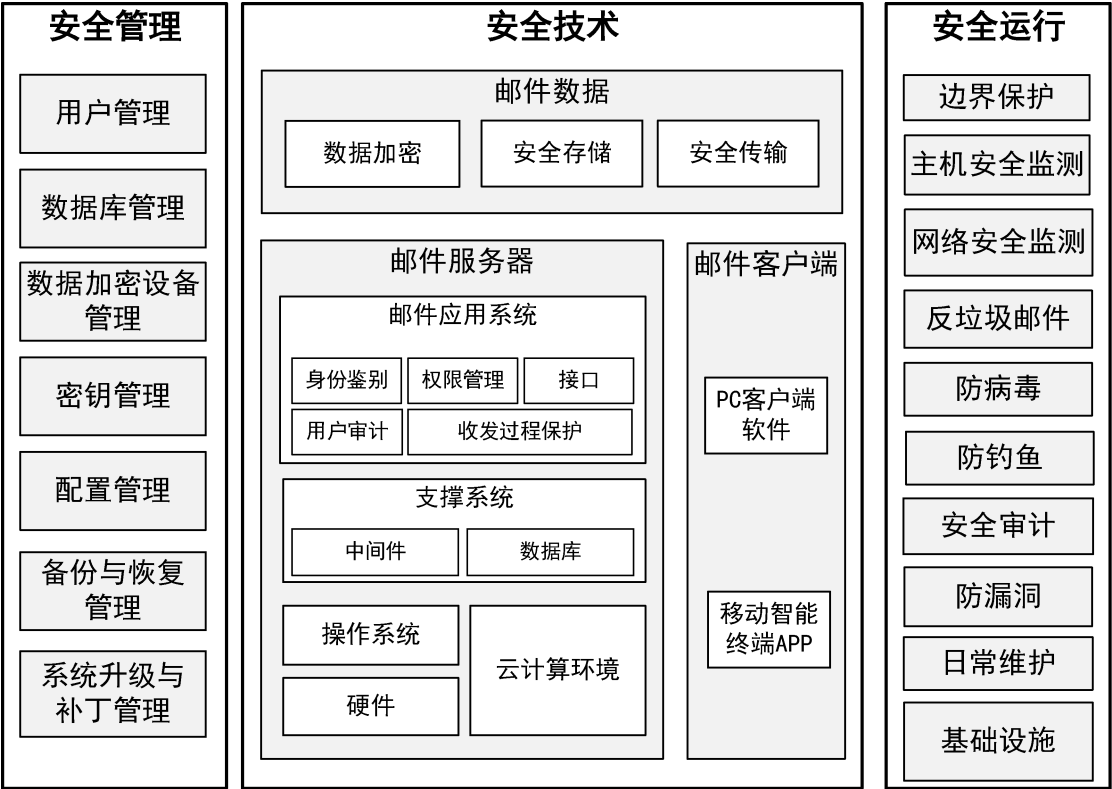


图 1 电子邮件系统安全技术框架

5.2 安全目标

电子邮件系统重点安全目标如下：

- a) 加强电子邮件系统的安全管控,降低电子邮件系统的安全风险；
- b) 通过加密技术来实现邮件数据在传输和存储中的保护,降低数据泄密的安全风险；
- c) 强化电子邮件系统身份鉴别安全措施,降低数据被窃取的风险；
- d) 规范安全管理措施和运行要求,构建完整的防御体系。

5.3 安全级别

本文件中,电子邮件系统的安全要求按其保障强度可划分为基本级和增强级两个等级的安全要求。各单位可根据本单位属性、用户数量和业务重要度选择使用基本级或增强级安全要求。电子邮件系统安全级别选择方法参见附录 A。

在本文件的技术要求中,黑体字表示基本级安全要求中未出现或增强级安全要求中加强的内容。

6 基本级安全要求

6.1 安全技术要求

6.1.1 邮件服务器

6.1.1.1 硬件

应符合 GB/T 39680—2020 要求。

6.1.1.2 操作系统

应符合 GB/T 20272—2026 第二级要求。

6.1.1.3 云计算环境

要求如下：

- a) 应符合 GB/T 31168—2023 一般要求；
- b) 云服务提供者、邮件系统运营者应根据 GB/T 31167—2023 履行相应管理责任。

6.1.1.4 支撑系统

6.1.1.4.1 中间件

应符合 GB/T 26232—2025 相关安全要求。

6.1.1.4.2 数据库

应符合 GB/T 20273—2019 第二级安全要求。

6.1.1.5 邮件应用系统

6.1.1.5.1 身份鉴别

要求如下。

- a) 应支持安全性增强的账户口令认证,包括:
 - 1) 当产品中存在默认口令时,在用户首次登录时提示用户对默认口令进行修改;
 - 2) 账户口令为字母、数字、符号的混用组合,且不少于 8 个字符;
 - 3) 具备账户口令自动审查功能,禁止使用弱口令;
 - 4) 账户口令设定有效期,超过有效期时,则不能登录;
 - 5) 具备口令防暴力破解功能,对 Web、POP3、SMTP 和 IMAP 等登录访问方式,当口令错误次数超过设定值后,应锁定该账户或禁止对应 IP 再次访问。
- b) 应具备身份鉴别异常处理功能,如采取限制登录错误次数等措施。
- c) 应具备异常登录情况识别,并对异常的登录行为进行报警,如同一时间段出现异地登录、多个 IP 同时登录同一账号、一个 IP 地址登录多个邮件账号等行为。
- d) 对于管理员账号,应采取访问控制策略,如对登录的 IP 地址段、登录设备等实施访问限制。
- e) 应具备超时认证的功能,当用户会话超时后,需进行重新认证。

6.1.1.5.2 权限管理

要求如下：

- a) 应具备用户分类功能,如分为管理员和邮件用户;
- b) 应能对各类用户赋予不同的权限;
- c) 应具备权限验证方法,采用技术手段,保证权限凭证数据不可伪造;
- d) 应在通过身份鉴别机制认证用户身份后,方可允许用户访问授权的功能;
- e) 应具备记录管理员访问过程操作日志的功能。

6.1.1.5.3 用户审计

要求如下：

- a) 应具备管理员行为审计功能,审计内容应包括:操作时间、管理员账户、登录 IP 地址、地理位置、登录方式、操作内容与结果等信息;
- b) 应具备邮件用户登录行为审计功能,审计内容应包括:登录时间、邮件用户账户、登录 IP 地址、地理位置、登录方式等信息;
- c) 应具备邮件用户发送邮件行为审计功能,审计内容应包括:发送时间、收件人、邮件主题、投递状态、是否撤回等信息;
- d) 应具备邮件用户接收邮件行为审计功能,审计内容应包括:收取时间、发件人、邮件主题、阅读状态等信息;
- e) 应具备邮件用户账户关键配置修改行为审计功能,审计内容应包括:时间、操作账户、修改内容、修改结果等信息;
- f) 审计数据至少保存一年。

6.1.1.5.4 接口

要求如下:

- a) 与第三方应用系统接口应采用身份鉴别机制,验证接口调用方身份的合法性;
- b) 与第三方应用系统接口的会话应设置生命周期,防止接口被恶意调用;
- c) 应对第三方应用系统接口调用的数据进行合法性检测,防止基于注入式、跨站请求伪造、模式验证、输入输出编码等攻击;
- d) 应对第三方应用系统接口设定资源使用权限,限定可访问的数据范围;
- e) 应具备记录接口调用过程操作日志的功能;
- f) 应向管理员明确系统所有接口,并标识区分内、外部接口;
- g) 应向管理员明确邮件系统用户、邮件组织用户、邮件审计用户、邮件安全用户、邮件用户接口。

6.1.1.5.5 收发过程保护

要求如下:

- a) 应具备邮件过滤功能,能接收或拒收指定域的邮件;
- b) 应默认关闭邮件中继功能,如需开启该功能,需配置相关安全策略,如能拒绝转发或仅转发来自指定 IP 地址或子网、目标为指定子网、来自指定域、来自指定邮件地址、来自指定用户名等邮件;
- c) 应具备邮件审批功能,能根据发件人、收件人、主题、内容、附件内容、附件格式等邮件特征,创建审批条件,满足审批条件的邮件,经审批员审批后,方能被投递/弹回/拒收(发)/转寄/抄送;
- d) 应具备支持 SPF、DKIM 机制检测邮件数据源的功能,能对发件人真实性进行检测,过滤发件人伪造的邮件;
- e) 应关闭邮件系统 SMTP 匿名转发功能;
- f) 应禁用或限制 VRFY、EXPN、TURN、SEND、SOML、SAML 等命令的使用;
- g) 如需使用中继节点转发邮件,邮件服务器应选择支持安全算法的 SSL/TLS 协议的中继节点;
- h) 应采用密码技术,保证中继节点无法获取邮件明文内容。

6.1.2 邮件客户端

6.1.2.1 邮件客户端通用要求

要求如下:

- a) 应默认启用 SSL/TLS 隧道、关闭自动转发等配置,用户变更默认配置时应予以提示;

- b) 应禁用将邮件用户账户身份认证相关凭证授权于未经本单位许可的第三方的服务或功能；
- c) 输入口令时,软件界面上不应显示明文口令；
- d) 应支持客户端软件完整性检测。

6.1.2.2 PC 客户端软件

要求如下：

- a) C/S 模式下应支持邮件加密、数字签名功能；
- b) C/S 模式下应支持邮件数据在本地加密存储；
- c) C/S 模式和 B/S 模式下均应支持基于 SSL/TLS 的邮件数据传输；
- d) C/S 模式和 B/S 模式运行环境均应有防病毒、木马的保护措施；
- e) 应支持证书验证,确保邮件服务器使用的 SSL/TLS 证书优先由国家密码管理部门认定的电子政务电子认证服务机构签发。

6.1.2.3 移动智能终端 APP

要求如下：

- a) 应用程序模式下应支持邮件加密、数字签名功能；
- b) 应用程序模式下应支持邮件数据在本地加密存储；
- c) 应用程序模式和 Web 模式下均应支持基于 SSL/TLS 的邮件数据传输；
- d) 应用程序模式和 Web 模式运行环境均应有防病毒、木马的保护措施；
- e) 应支持证书验证,确保邮件服务器使用的 SSL/TLS 证书优先由国家密码管理部门认定的电子政务电子认证服务机构签发。

6.1.3 邮件数据

6.1.3.1 数据加密

电子邮件数据在传输和存储过程中,须加密保护。要求如下：

- a) 邮件数据加密算法应符合国家密码管理部门的相关要求；
- b) 若使用数据加密设备实现数据加密,应符合下列要求：
 - 1) 应具备商用密码产品认证证书,且证书产品标准和技术要求应达到 GM/T 0028—2024 安全等级一级及以上；
 - 2) 应符合 GM/T 0018—2023 第 6 章关于设备接口描述的要求；
 - 3) 应采用加密技术,保证其与应用系统之间数据通信的安全性；
 - 4) 接口调用应支持 IP/MAC 地址绑定的访问控制机制；
 - 5) 应具备记录密码操作和管理日志的功能,并提供安全的日志审计接口。
- c) 邮件加密过程中的对称算法、非对称算法、摘要算法,宜优先使用国家商用密码算法,如使用对称算法进行内容加密,使用非对称算法进行数字信封的封装、数字签名等；
- d) 应符合 GB/T 32915—2026 关于随机性检测要求的规定；
- e) 应能根据邮件地址,安全获取邮件解密或签名使用的非对称密钥,该密钥不应写入无保护的可持续存储介质；
- f) 应使用不同的内容加密密钥加密邮件。

6.1.3.2 安全存储

要求如下：

- a) 应对存储的用户数据进行加密,包括:邮件数据、网盘文件、用户账号口令及个人信息等;
- b) 邮件账户口令若采用数字摘要方式存储,应具备随机性;
- c) 加密密钥更新后,应能对存储的历史加密数据进行解密。

6.1.3.3 安全传输

要求如下:

- a) 应支持安全算法的 SSL、TLS 协议,对传输数据进行加密;
- b) 应能验证客户端 SSL、TLS 证书的合法性。

6.2 安全管理要求

6.2.1 用户管理

6.2.1.1 用户分类管理

应按不同权限对用户进行分类,用户分类如下:

- a) 邮件系统用户,即系统管理员,是指能对邮件系统安全运行进行操作管理的用户;
- b) 邮件组织用户,即组织管理员,是指能对邮件用户进行增、删、改、查等操作的用户;
- c) 邮件审计用户,即审计管理员,是指能对邮件系统所有操作进行审计查看的用户;
- d) 邮件安全用户,即安全管理员,是指能对系统中的安全策略进行配置的用户;
- e) 邮件用户,即邮件使用用户,是指能进行邮件收发等操作的用户。

6.2.1.2 用户审计与管理

要求如下:

- a) 应对邮件系统用户进行审计;
- b) 应对邮件组织用户进行审计;
- c) 应对邮件审计用户进行审计;
- d) 应对邮件安全用户进行审计;
- e) 应对邮件用户进行审计;
- f) 应支持仅针对特定用户组或特定用户的审计;
- g) 邮件用户应由邮件组织用户创建,建立邮件用户的申请、发放、变更、注销等流程,严格账号审批登记,定期开展账号清理。

6.2.2 数据库管理

6.2.2.1 数据库管理系统用户标识与鉴别

要求如下:

- a) 访问邮件数据库管理系统的用户,应具有预先建立的标识;
- b) 邮件数据库管理系统应对登录用户的身份进行鉴别;
- c) 身份鉴别失败后,应根据失败次数与事件阈值采取相应措施,如锁定账户、禁用账户等。

6.2.2.2 数据库管理系统访问控制

要求如下:

- a) 应具有访问控制列表,阻止任何未经授权的访问,许可经过授权的访问;
- b) 应具备多权限管理员机制,如安全管理员、审计管理员、数据库管理员、系统管理员等。

6.2.2.3 数据库管理系统安全审计

要求如下：

- a) 应具有独立的系统审计员；
- b) 应具备对审计管理员分级、分组的功能，实现分级审计；
- c) 应提供完整全面的审计日志；
- d) 应具备日志保护机制，避免包括审计日志在内的各种日志信息被非法篡改、破坏或删除；
- e) 应支持对特定组或特定用户的审计；
- f) 审计内容应包括各类、各级管理员的登录及操作的具体内容，包括：时间、管理员用户名、管理动作等；
- g) 应支持对用户登录、操作行为的具体内容进行审计，如删除邮件的操作；
- h) 应支持对异常行为的审计，如管理员、普通用户的异常登录等。

6.2.2.4 数据库管理系统数据完整性

要求如下：

- a) 应提供相应的数据完整性保证机制；
- b) 应对数据完整性进行检验。

6.2.2.5 数据库管理系统数据机密性

应具有口令数据加密或其他保护措施，实现存储口令数据的机密性。

6.2.2.6 数据库管理系统数据备份和恢复

要求如下：

- a) 应具备本地数据备份与恢复功能，且支持完整备份和增量备份；
- b) 应具备异地数据备份机制，将数据定时批量备份到异地存储。

6.2.3 数据加密设备管理

应针对密码系统中各种密码设备的使用、管理、备份与恢复等，建立完善的安全管理制度。

6.2.4 密钥管理

要求如下：

- a) 所采用密码算法及密钥长度应符合国家密码管理部门相关规范要求；
- b) 密钥生成：内容加密密钥和用户身份鉴别密钥，其生成应有可靠的随机源，或采用经商用密码检测认证合格的密码产品；
- c) 密钥分发：内容加密密钥应使用收件人的公钥和非对称算法进行加密保护后，分发给收件人，收件人或签名人的公钥应通过可信方式获取；
- d) 密钥存储：内容加密密钥应由收件人公钥加密后储存于加密邮件数据中，解密或签名的私钥应存储在安全介质中或使用后即销毁；
- e) 密钥销毁：内容加密密钥在每次使用后应立即销毁；
- f) 密钥备份与恢复：应制定并实施密钥备份策略，确保密钥丢失或损坏时能恢复，同时备份过程应遵循相关安全策略，密钥恢复过程应经过多因子认证和审批，防止未授权访问；
- g) 密钥更新：应周期性地更新用户加密密钥。

6.2.5 配置管理

要求如下：

- a) 应具备分类管理控制机制,各类管理员仅允许其按照组织权限进行配置操作;
- b) 应具备按功能权限控制机制,各类管理员仅允许其按照功能权限进行配置操作;
- c) 应具备各类管理员账号绑定 IP 地址或 MAC 地址功能;
- d) 应具备配置信息备份和快速恢复功能;
- e) 应留存配置变更的操作日志,日志内容包括时间、登录 IP 地址、访问 IP 地址、操作账户、操作与结果等;
- f) 应提供配置快照功能,当配置发生变更时能自动生成快照,修改配置出错后可使配置信息恢复到出错前的快照状态。

6.2.6 备份与恢复管理

要求如下：

- a) 应具备数据备份机制,将数据进行本地、异地备份;
- b) 应能对数据进行完整备份和增量备份。

6.2.7 系统升级及补丁管理

要求如下：

- a) 应有明确的软件支持生命周期,对于软件每个版本应提供及时、持续的安全升级服务;
- b) 系统升级时应不产生业务中断事故;
- c) 系统升级失败时,应可卸载指定升级包,恢复历史版本;
- d) 应针对已被披露的漏洞及时修复;
- e) 应符合 GB/T 43698—2024 中 8.2 的要求;
- f) 若采用云计算环境,云服务提供者应负责识别其所提供的云上业务系统的漏洞,并及时进行修复,确保云服务的供应链安全。

6.3 安全运行要求

6.3.1 边界保护

要求如下：

- a) 应在电子邮件系统外围部署防火墙,并配置安全规则;
- b) 应对流转过程中的邮件传输协议进行分析,可采取阻断、记录或报警等操作。

6.3.2 主机安全监测

要求如下：

- a) 应进行服务器硬件、软件运行状态监测;
- b) 应能识别不符合协议规范的网络会话数据流,同时提取该会话所属进程的基本信息、远端 IP 地址;
- c) 应要求开发方提供系统业务运行时命令执行、进程调用、文件使用等情况,并支持实时监测。

6.3.3 网络安全监测

要求如下：

- a) 应配置专用的安全监测设备,以旁路接入方式部署在电子邮件系统出入口;
- b) 应要求开发方提供邮件系统用户、邮件组织用户、邮件审计用户、邮件安全用户、邮件用户允许访问的 Web 业务路径及接口等信息;
- c) 应对流转过程中的邮件是否符合编码标准进行监测,记录异常邮件内容并报警;
- d) 应对流转过程中的邮件附件进行监测,记录无法识别格式的附件并报警;
- e) 应进行木马植入攻击监测;
- f) 应进行隐蔽后门攻击监测;
- g) 应进行异常端口使用监测;
- h) 应进行邮件服务器网络异常通信行为监测;
- i) 应进行异常收发邮件行为监测;
- j) 应进行邮件服务器 Web 网页挂马攻击行为监测;
- k) 应进行邮件服务器 Web 网页隐藏、不可见链接攻击行为监测;
- l) 应支持通过关键词、语义识别等对邮件正文或附件内容进行监测,避免敏感信息经由邮件外发;
- m) 若采用云计算环境,云服务提供者应对所提供的云服务进行持续风险监测,并根据 GB/T 31168—2023 要求保证云服务的业务连续性。

6.3.4 反垃圾邮件

要求如下:

- a) 应符合 GB/T 30282—2023 中规定的有关要求;
- b) 应支持对来自本单位内部邮件账户发送的垃圾邮件的检测、拦截。

6.3.5 防病毒

要求如下:

- a) 应具备两种以上的防病毒引擎,至少包含一种启发式防病毒引擎;
- b) 应支持自定义规则查杀特定恶意程序;
- c) 应能对邮件正文及附件的整体进行病毒过滤;
- d) 应支持在线升级与离线升级病毒库;
- e) 应支持对来自本单位内部邮件账户发送的存在恶意病毒的邮件的检测、拦截;
- f) 对存在病毒的邮件,可设置拒绝发送或拒绝接收、在邮件中添加警告信息、不处理等操作;
- g) 应支持 GB/T 44886.4—2026 共享威胁信息。

6.3.6 防钓鱼

要求如下:

- a) 应支持通过域名、URL 链接比对技术,对发件人邮件域、正文或附件中的域名、URL 链接进行比对,以识别钓鱼、仿冒等有害邮件;
- b) 应支持通过关键词或语义识别技术,对邮件主题、正文或附件中的文字内容进行匹配,以识别钓鱼、仿冒等有害邮件;
- c) 对于邮件正文中指向外部网站的 URL 链接、短地址链接和图形二维码,用户点击打开前应发出风险提示;
- d) 对于邮件附件嵌入外部网站的 URL 链接、短地址链接和图形二维码,用户下载附件前应发出风险提示;
- e) 应支持设置域名、URL 链接黑名单,对正文、附件中出现的黑名单域名、URL 链接进行阻断;

- f) 应支持对来自本单位内部邮件账户发送的钓鱼邮件的检测、拦截；
- g) 应支持 GB/T 44886.4—2026 共享威胁信息。

6.3.7 安全审计

6.3.7.1 数据库操作审计

要求如下：

- a) 应记录和审计数据库 SQL 级操作，记录包括时间、数据库服务器名称、IP 地址、MAC 地址、端口号、用户名、操作执行结果及原始 SQL 语句；
- b) 应具备双向审计功能，即审计数据库客户端的访问行为，同时审计数据库的返回结果；
- c) 应能定义审计策略，策略元素至少包括时间、来源、角色、SQL 操作类型、事件类型、数据库 SQL 语句关键字、延迟时间、影响行数、异常串、基于数据库服务器组或者资产组；
- d) 应具备丰富的数据查询检索功能，能以数据库访问时间、IP 地址、端口号、用户名、操作类型、SQL 中的关键词等条件进行审计查询；
- e) 应具备数据库防攻击安全规则库，能根据预设置策略发现诸如 SQL 注入、已知数据库漏洞、口令猜解、缓冲区溢出等异常行为；
- f) 应具备权限预警功能，能针对最高权限滥用、误操作、恶意操作等行为进行报警和定位。

6.3.7.2 日志审计

要求如下：

- a) 应记录和审计操作系统安全日志；
- b) 应记录和审计 Web 中间件安全日志；
- c) 应记录和审计邮件系统接口调用过程操作日志；
- d) 应记录和审计邮件应用系统日志；
- e) 应按 6.2.2.3 中的要求实现数据库访问日志的记录与审计；
- f) 应记录和审计数据加密设备安全日志；
- g) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

6.3.8 防漏洞

要求如下：

- a) 应具备强制要求系统管理员修改默认口令、默认系统配置的功能；
- b) 应不存在已知安全漏洞，如：命令执行、SQL 注入、跨站脚本、越权访问、缓冲区溢出等；
- c) 若采用了第三方厂商的部件，该部件应不存在安全漏洞。

6.3.9 日常维护

要求如下：

- a) 应建立配套运维管理制度，包括明确维护人员的责任、系统维护和配置变更的审批、系统维护和配置变更过程的监督控制等；
- b) 系统管理员应定期检查和记录邮件系统运行状态，发现异常情况应及时上报主管领导；
- c) 系统管理员应定期修改邮件系统管理员口令；
- d) 系统管理员应定期对邮件系统进行漏洞检测、升级和加固系统；
- e) 邮件系统发生故障时，应按运维工作流程进行维护，并记录维护操作内容；
- f) 变更邮件系统配置时，应按运维工作流程进行操作，并记录配置变更内容；

- g) 不应在邮件系统(邮件客户端除外)中使用移动存储介质;
- h) 若采用云计算环境,应符合下列要求:
 - 1) 系统管理员按运维工作流程对云上业务系统进行运维审计,确保云服务的安全性、稳定性;
 - 2) 迁移与退出时,云服务提供者提供详细的存储、销毁、删除计划,确保有效擦除数据;
 - 3) 做好云内的安全策略配置和更新、云产品账号管理、访问授权、权限管理等。

6.3.10 基础设施

要求如下:

- a) 应保证邮件服务器基础设施位于中国境内;
- b) 若采用云计算环境,应保证邮件系统不能部署于低于其网络安全保护等级的云计算环境。

7 增强级安全要求

7.1 安全技术要求

7.1.1 邮件服务器

7.1.1.1 硬件

要求如下:

- a) 应符合 6.1.1.1 要求;
- b) 应使用符合相关国家政策与标准的 CPU 芯片、部件和设备。

7.1.1.2 操作系统

应符合 GB/T 20272—2026 第三级要求。

7.1.1.3 云计算环境

要求如下:

- a) 应符合 6.1.1.3 要求;
- b) 应符合 GB/T 31168—2023 增强要求。

7.1.1.4 支撑系统

7.1.1.4.1 中间件

应符合 6.1.1.4.1 要求。

7.1.1.4.2 数据库

应符合 GB/T 20273—2019 第三级安全要求。

7.1.1.5 邮件应用系统

7.1.1.5.1 身份鉴别

要求如下。

- a) 应符合 6.1.1.5.1 要求。
- b) 应采用双因子身份鉴别方式,且鉴别方式应至少符合以下一项要求:

- 1) 支持动态口令认证,动态口令可采用短信验证码或动态令牌等方式,短信验证码长度不小于6个字符并具有随机性,动态令牌产生符合GM/T 0021—2023中第5章关于动态口令生成方式的相关规定;
 - 2) 支持基于用户身份数字凭证的身份鉴别机制,若采用“挑战-应答”认证方式,挑战值具有随机性且不少于20个字节或为准确的时间戳,在验证签名过程中,系统验证签名密钥的有效性,在邮件传输协议中使用“挑战-应答”方式时,采用支持国家密码管理部门发布的非对称算法的扩展认证协议;
 - 3) 支持通过SSL/TLS协议双向认证模式来认证邮件客户端或浏览器客户端用户身份,系统验证邮件客户端或浏览器客户端证书的有效性;
 - 4) 支持通过国产商用密码技术进行身份认证,如通过运营商号码认证SDK进行身份认证、通过可信身份认证平台(CTID平台)进行身份认证。
- c) 应具备邮件客户端管理功能,支持邮件客户端准入、登记、取消授权等,可对于获得准入的客户端定期进行身份鉴别。

7.1.1.5.2 权限管理

要求如下:

- a) 应符合6.1.1.5.2要求;
- b) 应具备邮件用户访问过程操作日志。

7.1.1.5.3 用户审计

要求如下:

- a) 应符合6.1.1.5.3要求;
- b) 应具备邮件阅读、处理状态记录功能,内容包括时间、操作账户、登录IP地址、地理位置、登录方式、邮件主题等信息;
- c) 应具备邮件用户删除邮件行为审计功能,审计内容包括删除时间、发件人、邮件主题、删除方式等信息;
- d) 应具备邮件账户异常行为(如口令暴力破解、群发垃圾邮件、邮件账户异地登录及异常登录等)报警功能;
- e) 宜支持将审计数据保存时间延长至三年及以上;
- f) 应对审计进程进行保护,防止未经授权的中断。

7.1.1.5.4 接口

要求如下:

- a) 应符合6.1.1.5.4要求;
- b) 与第三方应用系统接口应采用加密技术,保证数据的机密性。

7.1.1.5.5 收发过程保护

应符合6.1.1.5.5要求。

7.1.2 邮件客户端

7.1.2.1 邮件客户端通用要求

要求如下:

- a) 应符合 6.1.2.1 要求；
- b) 邮件客户端软件应支持对邮件内容(含正文和附件)进行加密传输。

7.1.2.2 PC 客户端软件

要求如下：

- a) 应符合 6.1.2.2 要求；
- b) C/S 模式和 B/S 模式均应具备临时存储数据安全保护机制。

7.1.2.3 移动智能终端 APP

要求如下：

- a) 应符合 6.1.2.3 要求；
- b) 应用程序模式和 Web 模式均应具备临时存储数据的安全保护机制。

7.1.3 邮件数据

7.1.3.1 数据加密

电子邮件数据在传输和存储的过程中须加密保护,要求如下：

- a) 应符合 6.1.3.1 要求；
- b) 若使用数据加密设备实现数据加密,应具备商用密码产品认证证书,且证书产品标准和技术要求应达到 GM/T 0028—2024 安全等级二级及以上；
- c) 应支持可配置的加密密钥更新策略；
- d) 应支持灵活的加解密策略,可针对邮件组、收件人、发件人等应用个性化加解密策略。

基于加密技术的邮件系统模型参见附录 B。

7.1.3.2 安全存储

要求如下：

- a) 应符合 6.1.3.2 要求；
- b) 应对邮件处理过程中的暂存数据进行加密存储；
- c) 应符合 GB/T 39786—2021 第三级密码应用基本要求中关于数据存储的相关要求。

7.1.3.3 安全传输

要求如下：

- a) 应符合 6.1.3.3 要求；
- b) 应对邮件内容(含正文和附件)进行加密传输；
- c) SSL、TLS 协议应支持国家密码管理部门发布的相关算法标准；
- d) SSL、TLS 协议应优先采用国家密码管理部门认定的电子政务电子认证服务机构颁发的数字证书；
- e) 应符合 GB/T 39786—2021 第三级密码应用基本要求中关于数据传输的相关要求。

7.2 安全管理要求

7.2.1 用户管理

应符合 6.2.1 要求。

7.2.2 数据库管理

应符合 6.2.2 要求。

7.2.3 数据加密设备管理

应符合 6.2.3 要求。

7.2.4 密钥管理

应符合 6.2.4 要求。

7.2.5 配置管理

要求如下：

- a) 应符合 6.2.5 要求；
- b) 应具备对管理员操作终端访问控制机制，各类管理员仅允许通过特定操作终端进行配置操作。

7.2.6 备份与恢复管理

应符合 6.2.6 要求。

7.2.7 系统升级及补丁管理

应符合 6.2.7 要求。

7.3 安全运行要求

7.3.1 边界保护

应符合 6.3.1 要求。

7.3.2 主机安全监测

应符合 6.3.2 要求。

7.3.3 网络安全监测

应符合 6.3.3 要求。

7.3.4 反垃圾邮件

应符合 6.3.4 要求。

7.3.5 防病毒

应符合 6.3.5 要求。

7.3.6 防钓鱼

要求如下：

- a) 应符合 6.3.6 要求；
- b) 应支持对邮件正文及附件中出现的 URL 链接、短地址链接和图形二维码指向的页面进行安全检测，以识别钓鱼、仿冒等有害邮件。

7.3.7 安全审计

应符合 6.3.7 要求。

7.3.8 防漏洞

应符合 6.3.8 要求。

7.3.9 日常维护

应符合 6.3.9 要求。

7.3.10 基础设施

应符合 6.3.10 要求。

8 安全要求测试评价方法

8.1 安全技术要求测试评价方法

8.1.1 邮件服务器

8.1.1.1 硬件

测试评价方法如下。

a) 测试方法：

- 1) 按照 GB/T 39680—2020 第 6 章测评方法进行测试；
- 2) 查验服务器及其主要部件(CPU、内存、硬盘等)的原产地证明、供应商资质等信息,验证是否使用符合相关国家政策与标准的 CPU 芯片、部件和设备。

b) 预期结果：

- 1) 符合 GB/T 39680—2020 第 6 章预期结果；
- 2) 服务器硬件均使用符合相关国家政策与标准的 CPU 芯片、部件和设备。

c) 结果判定：

- 1) 若上述 1) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合；
- 2) 若上述 1)~2) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.1.1.2 操作系统

测试评价方法如下。

a) 测试方法：

- 1) 按照 GB/T 20272—2026 第二级要求测试评价方法进行测试；
- 2) 按照 **GB/T 20272—2026** 第三级要求测试评价方法进行测试。

b) 预期结果：

- 1) 符合 GB/T 20272—2026 第二级要求测试评价方法的预期结果；
- 2) 符合 **GB/T 20272—2026** 第三级要求测试评价方法的预期结果。

c) 结果判定：

- 1) 若上述 1) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否

则判定为不符合；

- 2) 若上述 2) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.1.1.3 云计算环境

测试评价方法如下。

a) 测试方法：

- 1) 查验所采用云服务商的云计算服务相应安全能力资质证明材料,验证其安全能力是否符合 GB/T 31168—2023 一般要求；
- 2) 查验相关合同、规章制度等文件,验证云服务提供者、邮件系统运营者是否根据 GB/T 31167—2023 要求履行相应管理责任；
- 3) 查验所采用云服务商的云计算服务相应安全能力资质证明材料,验证其安全能力是否符合 GB/T 31168—2023 增强要求。

b) 预期结果：

- 1) 符合 GB/T 31168—2023 一般要求；
- 2) 云服务提供者、邮件系统运营者根据 GB/T 31167—2023 要求履行相应管理责任；
- 3) 符合 GB/T 31168—2023 增强要求。

c) 结果判定：

- 1) 若上述 1)~2) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合；
- 2) 若上述 1)~3) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.1.1.4 支撑系统

8.1.1.4.1 中间件

测试评价方法如下。

a) 测试方法：

查验所采用中间件的安全配置或相关安全能力证明材料,验证中间件是否符合 GB/T 26232—2025 相关安全要求。

b) 预期结果：

符合 GB/T 26232—2025 相关安全要求。

c) 结果判定：

- 1) 若上述的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合；
- 2) 若上述的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.1.1.4.2 数据库

测试评价方法如下。

a) 测试方法：

- 1) 查验数据库相关安全能力证明材料,验证数据库是否符合 GB/T 20273—2019 第二级安全要求；

- 2) 查验数据库相关安全能力证明材料,验证数据库是否符合 GB/T 20273—2019 第三级安全要求。

b) 预期结果:

- 1) 符合 GB/T 20273—2019 第二级安全要求;
- 2) 符合 GB/T 20273—2019 第三级安全要求。

c) 结果判定:

- 1) 若上述 1) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 2) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.1.1.5 邮件应用系统

8.1.1.5.1 身份鉴别

测试评价方法如下。

a) 测试方法:

- 1) 查验邮件应用系统是否支持安全性增强的账户口令认证,包括口令强度筛查、口令自动审查、口令有效期筛查、口令防暴力破解,以及首次登录时的默认口令修改等内容;
- 2) 查验邮件应用系统是否具备身份鉴别异常处理功能,使用专用工具进行账号口令爆破,查验攻击行为是否受到限制;
- 3) 查验邮件应用系统是否具备异常登录识别功能,模拟邮件账号异地登录、多 IP 并发登录同一账号及单一 IP 登录多个账号等场景,验证是否能识别、标记异常情况并及时报警;
- 4) 查验对于管理员账号,是否采取访问控制策略,模拟管理员账号异常登录行为,如分别使用不同 IP 地址段、不同设备进行登录,验证管理员的异常登录行为是否受到访问限制;
- 5) 查验邮件应用系统是否具备超时认证功能,当用户会话超时后,验证是否需要重新进行身份认证;
- 6) 查验是否采用双因子身份鉴别方式,且鉴别方式是否至少符合以下一项要求:
 - 查验邮件应用系统是否支持短信验证码或动态令牌等动态口令认证方式,相关认证方式是否符合安全要求;
 - 查验邮件应用系统是否支持用户身份数字凭证的身份鉴别机制,相关身份鉴别机制是否符合安全要求;
 - 查验邮件应用系统是否支持通过 SSL/TLS 协议双向认证模式来认证邮件客户端或浏览器客户端用户身份,查验系统是否验证邮件客户端或浏览器客户端证书的有效性;
 - 查验是否支持通过国产商用密码技术进行身份认证,查验身份认证方式是否有效;
- 7) 查验邮件应用系统是否具备邮件客户端管理功能,查验是否可对获得准入的客户端定期进行身份鉴别。

b) 预期结果:

- 1) 具备首次登录时提示默认口令修改、口令强度筛查、口令自动审查、口令有效期筛查、口令防暴力破解等账户口令认证安全性增强功能;
- 2) 具备身份鉴别异常处理功能,口令爆破行为受到限制;
- 3) 具备异常登录识别功能,能识别、标记同一时间段出现异地登录、多个 IP 同时登录同一账号、一个 IP 地址登录多个邮件账号等异常登录情况并进行报警;

- 4) 对管理员账号采取了访问控制策略,管理员账号在规定登录 IP、登录设备以外的登录行为受到限制;
- 5) 具备超时认证功能,当用户会话超时后,需要重新进行身份认证;
- 6) 采用双因子身份鉴别方式,且鉴别方式至少符合以下一项要求:
 - 支持短信验证码或动态令牌等动态口令认证方式,短信验证码长度不小于 6 个字符并具有随机性,动态令牌产生符合 GM/T 0021—2023 中第 5 章关于动态口令生成方式的相关规定;
 - 支持基于用户身份凭证的身份鉴别机制,若采用“挑战-应答”认证方式,挑战值具有随机性且不少于 20 个字节或为准确的时间戳,在验证签名过程中,系统验证签名密钥的有效性,在邮件传输协议中使用“挑战-应答”方式时,采用支持国家密码管理部门发布的非对称算法的扩展认证协议;
 - 支持通过 SSL/TLS 协议双向认证模式来认证邮件客户端或浏览器客户端用户身份,系统验证邮件客户端或浏览器客户端证书的有效性;
 - 支持通过国产商用密码技术进行身份认证,身份认证方式有效;
- 7) 具备邮件客户端管理功能,支持邮件客户端准入、登记、取消授权等,可对于准入的客户端,配置定期身份鉴别策略。

c) 结果判定:

- 1) 若上述 1)~5) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~7) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.1.1.5.2 权限管理

测试评价方法如下。

a) 测试方法:

- 1) 查验邮件应用系统是否具备用户分类功能,支持对不同用户进行分类;
- 2) 查验邮件应用系统是否具备权限管理功能,是否对各类用户赋予不同权限;
- 3) 查验邮件应用系统是否具备权限验证方法,使用伪造或过期的权限凭证数据进行测试,验证是否通过系统权限验证;
- 4) 查验邮件应用系统是否具备访问控制策略,测试访问不同权限的资源是否需要身份鉴别;
- 5) 查验邮件应用系统是否具备记录管理员访问过程操作日志的功能,验证系统能否完整记录管理员的访问操作日志;
- 6) 查验邮件应用系统是否具备记录邮件用户访问过程操作日志的功能,验证系统能否完整记录邮件用户的访问操作日志。

b) 预期结果:

- 1) 具备用户分类功能,支持对不同用户进行分类,如分为管理员和邮件用户;
- 2) 具备权限管理功能,对各类用户赋予不同权限;
- 3) 具备权限验证方法,权限凭证数据不可伪造,伪造或过期的权限凭证数据无法通过系统权限验证;
- 4) 具备访问控制策略,用户通过身份鉴别机制认证后,方可访问授权的资源;
- 5) 具备记录管理员访问过程操作日志的功能,管理员的访问操作行为均被完整记录;
- 6) 具备记录邮件用户访问过程操作日志的功能,用户的访问操作行为均被完整记录。

c) 结果判定:

- 1) 若上述 1)~5) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~6) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.1.1.5.3 用户审计

测试评价方法如下。

a) 测试方法:

- 1) 查验邮件应用系统是否具备管理员行为审计功能,并查验其审计内容是否包括:操作时间、管理员账户、登录 IP 地址、地理位置、登录方式、操作内容与结果等信息;
- 2) 查验邮件应用系统是否具备用户登录行为审计功能,并查验其审计内容是否包括:登录时间、邮件用户账户、登录 IP 地址、地理位置、登录方式等信息;
- 3) 查验邮件应用系统是否具备邮件用户发送邮件行为审计功能,并查验其审计内容是否包括:发送时间、收件人、邮件主题、投递状态、是否撤回等信息;
- 4) 查验邮件应用系统是否具备邮件用户接收邮件行为审计功能,并查验其审计内容是否包括:收取时间、发件人、邮件主题、阅读状态等信息;
- 5) 查验邮件应用系统是否具备邮件用户账户关键配置修改行为审计功能,并查验其审计内容是否包括:时间、操作账户、修改内容、修改结果等信息;
- 6) 查验邮件应用系统的审计数据的留存期限以及相关管理制度对于审计数据的保存时间要求;
- 7) 查验邮件应用系统是否具备邮件阅读、处理状态记录功能,并查验其内容是否包括:时间、操作账户、登录 IP 地址、地理位置、登录方式、邮件主题等信息;
- 8) 查验邮件应用系统是否具备邮件用户删除邮件行为的审计功能,并查验其审计内容是否包括:删除时间、发件人、邮件主题、删除方式等信息;
- 9) 查验邮件应用系统是否具备邮件账户异常行为的报警功能,模拟口令暴力破解、群发垃圾邮件、邮件账户异地登录及异常登录等异常行为,验证报警是否及时准确;
- 10) 查验邮件应用系统的审计数据的留存期限以及相关管理制度对于审计数据的保存时间要求,验证审计数据保存时间是否为三年及以上;
- 11) 查验产品说明文档是否明确对审计进程进行保护,是否能防止未经授权的中断。

b) 预期结果:

- 1) 具备管理员行为审计功能,审计内容包括相应信息;
- 2) 具备邮件用户登录行为审计功能,审计内容包括相应信息;
- 3) 具备邮件用户发送邮件行为审计功能,审计内容包括相应信息;
- 4) 具备邮件用户接收邮件行为审计功能,审计内容包括相应信息;
- 5) 具备邮件用户账户关键配置修改行为审计功能,审计内容包括相应信息;
- 6) 邮件应用系统的审计数据至少保存一年;
- 7) 具备邮件阅读、处理状态记录功能,内容包括相应信息;
- 8) 具备邮件用户删除邮件行为的审计功能,审计内容包括相应信息;
- 9) 具备口令暴力破解、群发垃圾邮件、邮件账户异地登录及异常登录邮件账户等异常行为报警功能,报警及时准确;
- 10) 邮件应用系统的审计数据保存时间为三年及以上;
- 11) 产品说明文档中明确对审计进程进行保护,能防止未经授权的中断。

c) 结果判定:

- 1) 若上述 1)~6) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~9)、11) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合,预期结果 10) 为可选评估项。

8.1.1.5.4 接口

测试评价方法如下。

a) 测试方法:

- 1) 查验邮件应用系统与第三方应用系统接口是否采用身份鉴别机制,尝试访问相应接口获取数据,验证邮件应用系统是否验证接口调用方身份的合法性;
- 2) 查验邮件应用系统与第三方应用系统接口的会话是否设置生命周期,查看相关配置信息并进行测试,验证会话超过生命周期后是否可继续通过接口调用数据;
- 3) 查验邮件应用系统是否对第三方应用系统接口调用的数据进行合法性检测,进行攻击模拟测试,验证系统是否能检测并发现相关攻击行为;
- 4) 查验邮件应用系统是否对第三方应用系统接口设定资源使用限制,查看第三方应用系统接口的相关访问控制策略并进行测试,验证是否可根据访问控制策略限定可访问的数据范围;
- 5) 查验邮件应用系统是否具备记录接口调用过程操作日志的功能,模拟接口调用操作,验证系统是否完整记录接口调用过程操作日志;
- 6) 查验邮件应用系统是否向管理员明确系统所有接口并标识区分内、外部接口,查看相关说明文档,验证是否记录了系统所有接口信息以及相关信息是否明确、完整;
- 7) 查验邮件应用系统是否向管理员明确邮件系统用户、邮件组织用户、邮件审计用户、邮件安全用户、邮件用户接口,查看相关说明文档,验证是否记录了上述用户接口信息以及相关信息是否明确、完整;
- 8) 查验邮件应用系统与第三方应用系统接口是否采用加密技术。

b) 预期结果:

- 1) 与第三方应用系统接口采用身份鉴别机制,接口调用时验证接口调用方身份的合法性;
- 2) 与第三方应用系统接口的会话设置了生命周期,超过生命周期后无法继续通过接口调用数据,需要重新进行身份鉴别;
- 3) 对第三方应用系统接口调用的数据进行合法性检测,能防止基于注入式、跨站请求伪造、模式验证、输入输出编码等攻击;
- 4) 对第三方应用系统接口设定了资源使用限制,限定了可访问的数据范围;
- 5) 具备记录接口调用过程操作日志的功能,相关日志记录信息完整;
- 6) 向管理员明确系统所有接口,并标识区分内、外部接口,相关说明文档记录信息明确且完整;
- 7) 向管理员明确邮件系统用户、邮件组织用户、邮件审计用户、邮件安全用户、邮件用户接口,相关说明文档记录信息明确且完整;
- 8) 与第三方应用系统接口采用加密技术,可保证数据的机密性。

c) 结果判定:

- 1) 若上述 1)~7) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~8) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.1.1.5.5 收发过程保护

测试评价方法如下。

a) 测试方法：

- 1) 查验系统相关功能配置并通过不同域发送邮件进行测试,验证是否能接收或拒收指定域的邮件;
- 2) 查验系统相关功能配置,若采用邮件中继功能则进行测试,验证安全策略是否完善,如拒绝转发或仅转发来自指定 IP 地址或子网、目标为指定子网、来自指定域、来自指定邮件地址、来自指定用户名等邮件;
- 3) 使用不同域邮件测试账户分别向被测单位邮件系统测试账户发送测试邮件,以及使用被测单位邮件系统测试账户分别向不同域邮件测试账户发送测试邮件,验证是否能根据发件人、收件人、主题、内容、附件内容、附件格式等邮件特征创建审批条件,以及满足审批条件的测试邮件是否经审批员审批后方可被投递/弹回/拒收(发)/转寄/抄送;
- 4) 查验系统相关配置并发送发件人伪造的测试邮件,验证是否能通过 SPF、DKIM 机制过滤发件人伪造的测试邮件;
- 5) 查验邮件应用系统是否关闭邮件系统 SMTP 匿名转发功能;
- 6) 查验邮件应用系统是否禁用或限制 VRFY、EXPN、TURN、SEND、SOML、SAML 等命令的使用;
- 7) 查验邮件服务器是否使用中继节点转发邮件,如使用,测试相关中继节点是否支持安全算法的 SSL/TLS 协议;
- 8) 查阅产品说明文档是否明确支持采用密码技术对邮件内容加密,验证邮件系统是否启用相关加密策略保证中继节点无法获取邮件明文内容。

b) 预期结果：

- 1) 邮件应用系统具备邮件过滤功能,可接收或拒收指定域的邮件;
- 2) 邮件应用系统默认关闭邮件中继功能,如开启该功能,能拒绝转发或仅转发来自指定 IP 地址或子网、目标为指定子网、来自指定域、来自指定邮件地址、来自指定用户名等邮件;
- 3) 邮件应用系统具备邮件审批功能,能根据发件人、收件人、主题、内容、附件内容、附件格式等邮件特征,创建审批条件,满足审批条件的测试邮件,均需要审批员审批后,方能被投递/弹回/拒收(发)/转寄/抄送;
- 4) 邮件应用系统具备支持 SPF、DKIM 机制检测邮件数据源的功能,能对发件人真实性进行检测,过滤发件人伪造的邮件;
- 5) 邮件应用系统已关闭邮件系统 SMTP 匿名转发功能;
- 6) 邮件应用系统已禁用或限制 VRFY、EXPN、TURN、SEND、SOML、SAML 等命令的使用;
- 7) 如使用中继节点转发邮件,邮件服务器选择了支持安全算法的 SSL/TLS 协议的中继节点;
- 8) 产品说明文档明确支持采用密码技术对邮件内容加密,邮件系统启用相关加密策略,中继节点无法获取邮件明文内容。

c) 结果判定：

- 1) 若上述 1)~8) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~8) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.1.2 邮件客户端

8.1.2.1 邮件客户端通用要求

测试评价方法如下。

a) 测试方法：

- 1) 查验是否默认启用 SSL/TLS 隧道、关闭自动转发等配置并尝试变更默认配置,验证配置变更时是否予以提示;
- 2) 查验邮件客户端配置、邮件系统安全管理制度以及配套的检查、审计机制,验证邮件客户端是否禁用将邮件用户身份认证相关凭证授权于未经本单位许可的第三方的服务或功能、被测评单位是否存在明确的安全管理要求以及检查、审计机制是否完善;
- 3) 查验输入口令时,输入的字符是否被掩码字符代替;
- 4) 查验是否支持客户端软件完整性检测,尝试修改客户端软件的部分文件,验证软件是否能检测到变更并提示软件完整性受损;
- 5) 查验邮件客户端相关配置并进行邮件收发测试,验证是否支持对邮件内容(含正文和附件)进行加密传输。

b) 预期结果：

- 1) 默认启用 SSL/TLS 隧道、关闭自动转发等配置,尝试变更默认配置时,客户端予以提示;
- 2) 邮件客户端相关服务或功能已禁用,或被测评单位存在明确的安全管理要求并具备相应的检查、审计机制;
- 3) 输入口令时,输入的字符被掩码字符代替;
- 4) 支持客户端软件完整性检测,能检测到变更并提示软件完整性受损;
- 5) 存在相关加密配置,可实现对邮件内容(含正文和附件)进行加密传输。

c) 结果判定：

- 1) 若上述 1)~4) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~5) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.1.2.2 PC 客户端软件

测试评价方法如下。

a) 测试方法：

- 1) 查验 PC 客户端软件相关功能配置,并进行邮件加密、数字签名测试,验证 C/S 模式下是否支持邮件加密和数字签名;
- 2) 查验 PC 客户端软件相关功能配置,并进行本地加密存储测试,验证 C/S 模式下是否支持邮件数据在本地加密存储;
- 3) 查验 PC 客户端软件相关功能配置,并分别通过 C/S 模式和 B/S 模式进行邮件收发测试,验证是否支持基于 SSL/TLS 的邮件数据传输;
- 4) 查验相关安全管理制度,验证是否要求邮件用户 PC 安装防病毒、木马软件并及时更新病毒库,抽查部分 PC,验证是否安装防病毒、木马软件以及病毒库是否及时更新;
- 5) 查验是否支持证书验证,是否能识别邮件服务器的 SSL/TLS 证书是否由国家密码管理部门认定的电子政务电子认证服务机构签发;
- 6) 查验涉及临时存储数据安全保护机制的相关材料,验证 C/S 模式和 B/S 模式是否具备临

时存储数据的安全保护机制。

b) 预期结果：

- 1) C/S 模式下支持邮件加密和数字签名功能,相关功能合理、有效;
- 2) C/S 模式下支持邮件数据本地加密存储功能,相关测试数据已加密;
- 3) C/S 模式和 B/S 模式下均支持基于 SSL/TLS 的邮件数据传输;
- 4) C/S 和 B/S 模式运行环境均有防病毒、木马的保护措施,相关管理制度要求邮件用户 PC 安装防病毒、木马软件并及时更新病毒库,抽查的 PC 均安装防病毒、木马软件,病毒库已及时更新;
- 5) 支持证书验证,如当邮件服务器使用的 SSL/TLS 证书由国家密码管理部门认定的电子政务电子认证服务机构签发时,客户端有相关标识;
- 6) **C/S 模式和 B/S 模式具备临时存储数据安全保护机制。**

c) 结果判定：

- 1) 若上述 1)~5) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~6) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.1.2.3 移动智能终端 APP

测试评价方法如下。

a) 测试方法：

- 1) 查验移动智能终端 APP 相关功能配置,并进行邮件加密、数字签名测试,验证应用程序模式是否支持邮件加密和数字签名;
- 2) 查验移动智能终端 APP 相关功能配置,并进行本地加密存储测试,验证应用程序模式下是否支持邮件数据在本地加密存储;
- 3) 查验移动智能终端 APP 相关功能配置,并分别通过应用程序模式和 Web 模式进行邮件收发测试,验证是否支持基于 SSL/TLS 的邮件数据传输;
- 4) 查验相关安全管理制度,验证是否要求邮件用户移动智能终端安装防病毒、木马软件并及时更新病毒库,抽查部分移动智能终端,验证是否安装防病毒、木马软件以及病毒库是否及时更新;
- 5) 查验是否支持证书验证,是否能识别邮件服务器的 SSL/TLS 证书是否由国家密码管理部门认定的电子政务电子认证服务机构签发;
- 6) 查验涉及临时存储数据安全保护机制的相关材料,验证应用程序模式和 Web 模式是否具备临时存储数据的安全保护机制。

b) 预期结果：

- 1) 应用程序模式下支持邮件加密和数字签名功能,相关功能合理、有效;
- 2) 应用程序模式下支持邮件数据本地加密存储功能,相关测试数据已加密;
- 3) 应用程序模式和 Web 模式下均支持基于 SSL/TLS 的邮件数据传输;
- 4) 应用程序模式和 Web 模式运行环境均有防病毒、木马的保护措施,相关管理制度要求邮件用户移动智能终端安装防病毒、木马软件并及时更新病毒库,抽查的移动智能终端均安装防病毒、木马软件,病毒库已及时更新;
- 5) 支持证书验证,如当邮件服务器使用的 SSL/TLS 证书由国家密码管理部门认定的电子政务电子认证服务机构签发时,客户端有相关标识;
- 6) **应用程序模式和 Web 模式均具备临时存储数据的安全保护机制。**

c) 结果判定：

- 1) 若上述 1)~5) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合；
- 2) 若上述 1)~6) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.1.3 邮件数据

8.1.3.1 数据加密

测试评价方法如下。

a) 测试方法：

- 1) 查验邮件数据在传输和存储过程中是否进行加密,查验邮件服务器使用的加密算法,验证加密使用的算法是否符合国家密码管理部门的相关要求；
- 2) 若使用数据加密设备实现数据加密,查验是否符合以下要求：
 - 查验是否具备商用密码产品认证证书,验证证书产品标准和技术要求是否达到 GM/T 0028—2024 安全等级一级及以上；
 - 查验是否符合 GM/T 0018—2023 第 6 章关于设备接口描述的要求；
 - 查验是否采用加密技术,是否能保证其与应用系统之间数据通信的安全性；
 - 查验接口调用的访问控制机制,验证是否支持 IP/MAC 地址绑定的访问控制机制；
 - 查验是否具备记录密码操作和管理日志的功能,是否提供安全的日志审计接口。
- 3) 查验邮件加密过程中的对称算法、非对称算法、摘要算法是否使用国家商用密码算法,如使用对称算法进行内容加密,使用非对称算法进行数字信封的封装、数字签名等；
- 4) 查验涉及加密使用的随机数的随机性的相关材料,验证是否符合国家标准 GB/T 32915—2026 关于随机性检测要求的规定；
- 5) 查验邮件服务器进行邮件解密或签名的相关材料或配置,以及密钥存储管理相关要求,验证是否能根据邮件地址安全获取邮件解密或签名使用的非对称密钥,且相关密钥不应写入无保护的可持续存储介质；
- 6) 查验产品说明文档或系统配置是否支持使用不同的内容加密密钥加密邮件；
- 7) 若使用数据加密设备实现国家商用密码算法,查验是否具备商用密码产品认证证书,验证证书产品标准和技术要求是否达到 GM/T 0028—2024 安全等级二级及以上；
- 8) 查验是否支持可配置的密钥更新策略,验证密钥更新策略的有效性；
- 9) 查验是否支持灵活的加解密策略,是否可针对邮件组、收件人、发件人等应用个性化加解密策略。

b) 预期结果：

- 1) 邮件数据在传输和存储过程中均进行加密,且加密使用的算法符合国家密码管理部门的相关要求；
- 2) 若使用数据加密设备实现数据加密,符合以下要求：
 - 具备商用密码产品认证证书,且证书产品标准和技术要求达到 GM/T 0028—2024 安全等级一级及以上；
 - 符合 GM/T 0018—2023 第 6 章关于设备接口描述的要求；
 - 采用加密技术,能保证其与应用系统之间数据通信的安全性；
 - 接口调用支持 IP/MAC 地址绑定的访问控制机制；
 - 具备记录密码操作和管理日志的功能,能提供安全的日志审计接口；

- 3) 邮件加密过程中的对称算法、非对称算法、摘要算法均使用国家商用密码算法;
 - 4) 加密使用的随机数的随机性符合 GB/T 32915—2026 关于随机性检测的要求;
 - 5) 可根据邮件地址,安全获取邮件解密或签名使用的非对称密钥,该密钥未写入无保护的可持续存储介质;
 - 6) 邮件系统使用不同的内容加密密钥加密邮件;
 - 7) 若使用数据加密设备实现国家商用密码算法,具备商用密码产品认证证书,且产品标准和
技术要求达到 GM/T 0028—2024 安全等级二级及以上;
 - 8) 支持可配置的密钥更新策略,密钥更新策略有效;
 - 9) 支持灵活的加解密策略,可针对邮件组、收件人、发件人等应用个性化加解密策略。
- c) 结果判定:
- 1) 若上述 1)~2)、4)~6)的实际测试结果与对应的预期结果均一致,则判定为符合基本级
安全要求,否则判定为不符合,预期结果 3)为可选评估项;
 - 2) 若上述 1)~2)、4)~9)的实际测试结果与对应的预期结果均一致,则判定为符合增强级
安全要求,否则判定为不符合,预期结果 3)为可选评估项。

8.1.3.2 安全存储

测试评价方法如下。

- a) 测试方法:
- 1) 查验邮件系统存储的用户数据是否进行加密,加密数据类型是否包括邮件数据、网盘文
件、用户账号口令及个人信息等;
 - 2) 查验邮件账户口令的存储方式是否采用数字摘要方式存储,若使用,查验其配置策略,验
证其是否具备随机性;
 - 3) 加密密钥更新后,测试历史加密数据的解密功能是否正常;
 - 4) 查验产品说明文档或系统配置,验证是否对邮件处理过程中的暂存数据进行加密存储;
 - 5) 查验邮件系统数据加密存储相关安全能力证明材料,验证是否符合 GB/T 39786—2021
第三级密码应用基本要求中关于数据传输的相关要求。
- b) 预期结果:
- 1) 存储的用户数据已进行加密,包括邮件数据、网盘文件、用户账号口令及个人信息等;
 - 2) 邮件账户口令的存储方式若采用数字摘要方式存储,具备随机性;
 - 3) 加密密钥更新后,历史加密数据的解密功能正常;
 - 4) 对邮件处理过程中的暂存数据进行加密存储;
 - 5) 符合 GB/T 39786—2021 第三级密码应用基本要求中关于数据存储的相关要求。
- c) 结果判定:
- 1) 若上述 1)~3)的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要
求,否则判定为不符合;
 - 2) 若上述 1)~5)的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要
求,否则判定为不符合。

8.1.3.3 安全传输

测试评价方法如下。

- a) 测试方法:
- 1) 查验邮件系统支持的 SSL、TLS 协议版本,并尝试通过相应 SSL、TLS 协议进行邮件的收
发测试,验证是否对传输数据进行加密;

- 2) 查验是否支持验证客户端 SSL、TLS 证书的合法性,分别在客户端使用过期、非法、合法及无证书场景下进行测试,验证邮件系统是否可正常提供服务;
 - 3) 查验邮件服务器相关邮件传输安全策略,并进行邮件收发测试,验证邮件内容(包括正文和附件)在传输过程中是否进行加密;
 - 4) 查验邮件系统 SSL、TLS 配置选项,验证是否支持国家密码管理部门发布的相关算法标准;
 - 5) 查验邮件系统 SSL、TLS 协议采用的数字证书,验证数字证书是否由国家密码管理部门认定的电子政务电子认证服务机构颁发,如不是,验证数字证书的颁发机构是否可信;
 - 6) 查验邮件系统数据传输相关安全能力证明材料,验证是否符合 GB/T 39786—2021 第三级密码应用基本要求中关于数据传输的相关要求。
- b) 预期结果:
- 1) 邮件系统支持安全算法的 SSL、TLS 协议,对传输数据进行加密;
 - 2) 支持验证客户端 SSL、TLS 证书的合法性,无证书、证书非法或过期时,邮件服务不可用,仅在提供合法证书时,邮件服务可用;
 - 3) 邮件系统已配置邮件加密传输安全策略,相关测试邮件的邮件内容(包括正文和附件)在传输过程中均已进行加密;
 - 4) SSL、TLS 协议支持国家密码管理部门发布的相关算法标准;
 - 5) 采用由国家密码管理部门认定的电子政务电子认证服务机构颁发的数字证书,或采用其他可信机构颁发的数字证书;
 - 6) 符合 GB/T 39786—2021 第三级密码应用基本要求中关于数据传输的相关要求。
- c) 结果判定:
- 1) 若上述 1)~2) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
 - 2) 若上述 1)~6) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.2 安全管理要求测试评价方法

8.2.1 用户管理

8.2.1.1 用户分类管理

测试评价方法如下。

- a) 测试方法:
- 1) 查验系统后台或管理界面,确认是否按照不同权限对用户进行分类,包括邮件系统用户(系统管理员)、邮件组织用户(组织管理员)、邮件审计用户(审计管理员)、邮件安全用户(安全管理员)和邮件用户(邮件使用用户);
 - 2) 使用邮件系统用户登录,查验权限分配是否合理,是否能执行系统安全运行相关的操作管理,如系统配置修改、系统升级、备份与恢复等;
 - 3) 使用邮件组织用户登录,查验权限分配是否合理,是否能进行用户管理操作,如增加新用户、删除用户、修改用户信息和查询用户列表等;
 - 4) 使用邮件审计用户登录,查验权限分配是否合理,是否能查看邮件系统的所有操作日志,如登录记录、邮件收发记录及系统管理活动等;
 - 5) 使用邮件安全用户登录,查验权限分配是否合理,是否能对系统中的安全策略进行配置,如设置安全策略参数、对主体进行授权、配置可信验证策略等;

- 6) 使用邮件用户登录,查验权限分配是否合理,是否能进行邮件的接收、发送、草稿保存、附件上传下载等基本操作。

b) 预期结果:

- 1) 已按照不同权限对用户进行分类,包括邮件系统用户(系统管理员)、邮件组织用户(组织管理员)、邮件审计用户(审计管理员)、邮件安全用户(安全管理员)和邮件用户(邮件使用用户);
- 2) 权限分配合理,能执行系统安全运行相关的操作管理,如系统配置修改、系统升级、备份与恢复等;
- 3) 权限分配合理,能对邮件用户进行增、删、改、查等操作;
- 4) 权限分配合理,能查看邮件系统的所有操作日志,如登录记录、邮件收发记录及系统管理活动等;
- 5) 权限分配合理,能对系统中的安全策略进行配置,如设置安全策略参数、对主体进行授权、配置可信验证策略等;
- 6) 权限分配合理,能进行邮件的接收、发送、草稿保存、附件上传下载等基本操作。

c) 结果判定:

- 1) 若上述 1)~6) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~6) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.2.1.2 用户审计与管理

测试评价方法如下。

a) 测试方法:

- 1) 登录邮件系统用户账户并进行操作测试,验证审计日志是否准确记录了该邮件系统用户的行为;
- 2) 登录邮件组织用户账户并进行操作测试,验证审计日志是否准确记录了该邮件组织用户的行为;
- 3) 登录邮件审计用户账户并进行操作测试,验证审计日志是否准确记录了该邮件审计用户的行为;
- 4) 登录邮件安全用户账户并进行操作测试,验证审计日志是否准确记录了该邮件安全用户的行为;
- 5) 登录邮件用户账户并进行操作测试,查验审计日志是否准确记录了该邮件用户的行为;
- 6) 查验审计策略,登录特定用户组或特定用户进行操作测试,验证审计日志是否可聚焦并准确记录该特定用户组或特定用户的行为;
- 7) 测试执行邮件用户账号创建操作,查验邮件用户账号创建是否只能由邮件组织用户完成,查验是否具有邮件用户的申请、发放、变更、注销等流程,验证账号审批登记是否严格,是否定期开展账户清理工作。

b) 预期结果:

- 1) 可对邮件系统用户进行审计,测试行为均被准确记录;
- 2) 可对邮件组织用户进行审计,测试行为均被准确记录;
- 3) 可对邮件审计用户进行审计,测试行为均被准确记录;
- 4) 可对邮件安全用户进行审计,测试行为均被准确记录;
- 5) 可对邮件用户进行审计,测试行为均被准确记录;

- 6) 支持对特定用户组或特定用户的审计,测试行为均被准确记录;
 - 7) 邮件用户账号创建只能由邮件组织用户完成,具有邮件用户的申请、发放、变更、注销等流程,严格进行账号审批登记,定期对账号开展清理工作。
- c) 结果判定:
- 1) 若上述 1)~7)的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
 - 2) 若上述 1)~7)的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.2.2 数据库管理

8.2.2.1 数据库管理系统用户标识与鉴别

测试评价方法如下。

- a) 测试方法:
- 1) 查验访问邮件数据库管理系统的用户是否具有预先建立的唯一身份标识;
 - 2) 查验邮件数据库管理系统是否能对登录用户的身份进行鉴别,使用不同权限的测试账户登录邮件数据库管理系统,验证是否对登录用户的身份进行鉴别以及鉴别机制是否有效;
 - 3) 查验身份鉴别失败后,是否根据失败次数与事件阈值采取相应措施,使用不同权限的测试账户进行口令爆破,验证是否根据失败次数与事件阈值采取相应措施,如锁定账户、禁用账户等。
- b) 预期结果:
- 1) 访问邮件数据库管理系统的用户具有预先建立的唯一身份标识;
 - 2) 邮件数据库管理系统能对登录用户的身份进行鉴别,鉴别成功时可进行相应的系统操作、鉴别失败时禁止用户访问;
 - 3) 身份鉴别失败后,能根据失败次数与事件阈值采取相应措施,如锁定账户、禁用账户等。
- c) 结果判定:
- 1) 若上述 1)~3)的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
 - 2) 若上述 1)~3)的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.2.2.2 数据库管理系统访问控制

测试评价方法如下。

- a) 测试方法:
- 1) 查验是否具有访问控制列表,使用测试账户进行访问,验证是否能阻止任何未经授权的访问,许可经过授权的访问;
 - 2) 查验数据库管理系统提供方的技术文档,验证是否具备多权限管理员机制,使用不同权限的测试账户登录数据库管理系统,验证权限分配是否合理。
- b) 预期结果:
- 1) 具有访问控制列表,能阻止任何未经授权的访问,许可经过授权的访问;
 - 2) 具备多权限管理员机制,如安全管理员、审计管理员、数据库管理员、系统管理员等,各管理员权限分配合理。
- c) 结果判定:

- 1) 若上述 1)~2) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~2) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.2.2.3 数据库管理系统安全审计

测试评价方法如下。

a) 测试方法:

- 1) 查验是否具有独立的系统审计员;
- 2) 查验是否具备对审计管理员分级、分组的功能,分别登录不同权限的审计管理员进行测试,验证是否实现分级审计;
- 3) 查验审计日志中相关字段和内容是否完整、全面;
- 4) 查验是否具备日志保护机制,尝试非法修改、破坏或删除包括审计日志在内的各种日志信息,验证是否不能被非法篡改、破坏或删除;
- 5) 查验是否支持对特定组或特定用户进行审计;
- 6) 查验审计日志,审计内容是否包括各类、各级管理员的登录、操作的具体内容;
- 7) 查验是否支持对用户登录、操作行为的具体内容进行审计,使用不同权限的测试账户进行删除测试邮件等操作,验证相应的操作行为信息是否被完整记录并支持审计;
- 8) 查验是否支持对异常行为的审计,使用不同权限的测试账户进行异常行为操作,验证相应的异常行为信息是否被完整记录并支持审计。

b) 预期结果:

- 1) 具有独立的系统审计员;
- 2) 具备对审计管理员分级、分组的功能,能实现分级审计;
- 3) 审计日志中相关字段和内容完整、全面;
- 4) 具备日志保护机制,包括审计日志在内的各种日志信息不能被非法篡改、破坏或删除;
- 5) 支持对特定组或特定用户进行审计;
- 6) 审计内容包括各类、各级管理员的登录及操作的具体内容,包括:时间、管理员用户名、管理动作等;
- 7) 支持对用户登录、各种操作行为的具体内容进行审计,测试账户的操作行为信息均被完整记录并支持审计;
- 8) 支持对异常行为的审计,测试账户的异常行为信息均被完整记录并支持审计。

c) 结果判定:

- 1) 若上述 1)~8) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~8) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.2.2.4 数据库管理系统数据完整性

测试评价方法如下。

a) 测试方法:

- 1) 查验数据库管理系统完整性保证机制相关安全能力证明材料,验证数据完整性保证机制是否有效;
- 2) 查验是否对数据完整性进行检验,包括但不限于数据完整性检验日志、记录等。

- b) 预期结果:
 - 1) 具有数据完整性保证机制,能确保数据在存储过程中不被非法修改、破坏,保证数据的完整性;
 - 2) 可对数据完整性进行检验,存在数据完整性检验日志、记录。
- c) 结果判定:
 - 1) 若上述 1)~2)的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
 - 2) 若上述 1)~2)的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.2.2.5 数据库管理系统数据机密性

测试评价方法如下。

- a) 测试方法:查验是否具有口令数据加密或其他保护措施,登录数据库管理系统,验证口令数据是否采用加密储存或其他保护措施。
- b) 预期结果:具有口令数据加密或其他保护措施,能实现存储密码数据的机密性。
- c) 结果判定:
 - 1) 若上述实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
 - 2) 若上述实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.2.2.6 数据库管理系统数据备份和恢复

测试评价方法如下。

- a) 测试方法:
 - 1) 查验数据库管理系统相关功能配置以及备份与恢复日志记录,验证是否具备本地数据备份与恢复功能,是否支持完整备份和增量备份;
 - 2) 查验数据库管理系统数据备份相关配置以及数据备份记录,验证是否具备将数据定时批量备份到异地存储的异地数据备份机制。
- b) 预期结果:
 - 1) 具备本地数据备份与恢复功能,且支持完整备份和增量备份;
 - 2) 具备异地数据备份机制,已将数据定时批量备份到异地存储。
- c) 结果判定:
 - 1) 若上述 1)~2)的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
 - 2) 若上述 1)~2)的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.2.3 数据加密设备管理

测试评价方法如下。

- a) 测试方法:查验邮件系统所涉及的密码设备的相关安全管理制度,验证是否对相关密码设备的使用、管理、备份与恢复等建立完善的安全管理制度。
- b) 预期结果:安全管理制度完善,包括对密码系统中各种密码设备的使用、管理、备份与恢复等要求。

c) 结果判定:

- 1) 若上述实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.2.4 密钥管理

测试评价方法如下。

a) 测试方法:

- 1) 查验所采用密钥的配置信息,验证密码算法及密钥长度是否符合国家密码管理部门相关规范要求;
- 2) 查验涉及电子邮件系统的相关材料是否涵盖了密钥的全生命周期管理,包括密钥生成、分发、存储、使用、更新、销毁、备份与恢复,以及各个环节是否符合相关要求;
- 3) 若使用密码产品实现密钥管理,查验所使用的密码产品是否已获得国家密码管理部门认证的产品证书,且提供的产品形态是否与原证书备案描述一致。

b) 预期结果:

- 1) 所采用密码算法及密钥长度符合国家密码管理部门相关规范要求;
- 2) 具备密钥全生命周期管理机制,包括密钥生成、分发、存储、使用、更新、销毁及备份与恢复且各个环节符合相关要求;
- 3) 若使用密码产品实现密钥管理,所使用的密码产品已获得国家密码管理部门认证的产品证书,且提供的产品形态与原证书备案描述一致。

c) 结果判定:

- 1) 若上述 1)~3) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~3) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.2.5 配置管理

测试评价方法如下。

a) 测试方法:

- 1) 查验是否具备按组织权限进行配置管理的控制机制,使用各类管理员测试账号登录系统进行配置操作,验证是否仅允许在组织权限内进行配置;
- 2) 查验是否具备按功能权限进行配置管理的控制机制,使用各类管理员测试账号登录系统进行配置操作,验证是否仅允许在功能权限内进行配置;
- 3) 查验是否具备绑定 IP 地址或 MAC 地址功能,测试账号绑定 IP 地址或 MAC 地址后,使用其他 IP 地址或 MAC 地址登录该测试账号,验证是否能正常登录;
- 4) 查验是否具备配置信息备份和快速恢复功能,尝试对配置信息进行备份和快速恢复,验证相关功能是否有效;
- 5) 查验是否具备配置变更操作日志,使用各类管理员测试账号登录后进行配置变更,验证是否留存了配置变更的操作日志,包括但不限于时间、登录 IP 地址、访问 IP 地址、操作账户、操作与结果等;
- 6) 查验是否具备配置快照功能,使用各类管理员测试账号登录后进行配置变更,验证是否能自动生成快照,以及是否能通过快照恢复到出错前的快照状态;

- 7) 查验是否具备对管理员操作终端的访问控制机制,分别使用不同的操作终端尝试登录管理员账号,验证是否仅允许通过特定操作终端进行配置操作。

b) 预期结果:

- 1) 具备按组织权限进行配置管理的控制机制,各类管理员仅允许在组织权限内进行配置;
- 2) 具备按功能权限进行配置管理的控制机制,各类管理员仅允许在功能权限内进行配置;
- 3) 具备绑定 IP 地址或 MAC 地址功能,非绑定 IP 地址或 MAC 地址登录测试账号被禁止登录;
- 4) 具备配置信息备份和快速恢复功能,备份和快速恢复功能有效;
- 5) 具备配置变更操作日志,配置变更均有日志记录,且日志记录信息要素无缺失,包括但不限于时间、登录 IP 地址、访问 IP 地址、操作账户、操作与结果等;
- 6) 具备配置快照功能,配置变更可自动生成快照,可通过快照恢复到出错前的快照状态;
- 7) 具备对管理员操作终端的访问控制机制,仅允许通过特定操作终端进行配置操作。

c) 结果判定:

- 1) 若上述 1)~6) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~7) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.2.6 备份与恢复管理

测试评价方法如下。

a) 测试方法:

- 1) 查验数据备份机制的有效性,包括备份的触发机制、备份数据的完整性和一致性、备份恢复过程的可行性和准确性,验证是否按照数据备份机制对数据进行本地、异地备份;
- 2) 查验能否对数据进行完整备份和增量备份,数据备份机制是否有效。

b) 预期结果:

- 1) 按照数据备份机制对数据进行本地、异地备份,数据备份机制有效;
- 2) 能对数据进行完整备份和增量备份,数据备份机制有效。

c) 结果判定:

- 1) 若上述 1)~2) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~2) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.2.7 系统升级及补丁管理

测试评价方法如下。

a) 测试方法:

- 1) 查验是否具有明确的软件支持生命周期,查看相关管理制度、软件供应商支撑材料以及系统版本升级记录等,验证对于软件每个版本是否提供及时、持续的安全升级服务;
- 2) 查验系统升级时是否不会产生业务中断事故,查看系统升级记录与运行记录,验证系统是否存在业务中断事故;
- 3) 查验是否建立系统回退机制和流程,并依据系统回退机制和流程执行,查验是否留存相关记录,包括但不限于回退预案、记录等;
- 4) 查验是否建立漏洞处理机制,并依据漏洞处理机制执行,查验是否及时修复漏洞;

- 5) 查验相关合同、管理制度等证明材料,验证是否符合 GB/T 43698—2024 中 8.2 的要求;
 - 6) 若采用云计算环境,查验相关合同、管理制度、漏洞修复记录等证明材料,验证云服务提供者是否负责识别其所提供的云上业务系统的漏洞,是否对漏洞及时进行修复。
- b) 预期结果:
- 1) 有明确的软件支持生命周期,对于软件每个版本可提供及时、持续的安全升级服务;
 - 2) 系统升级时未产生业务中断事故;
 - 3) 建立了系统回退机制和流程,系统升级失败时,可卸载指定升级包,恢复历史版本;
 - 4) 建立了漏洞处理机制,针对已被披露的漏洞及时修复;
 - 5) 符合 GB/T 43698—2024 中 8.2 供应活动管理相关要求;
 - 6) 若采用云计算环境,云服务提供者负责识别其所提供的云上业务系统的漏洞,能对漏洞及时进行修复。
- c) 结果判定:
- 1) 若上述 1)~6) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
 - 2) 若上述 1)~6) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.3 安全运行要求测试评价方法

8.3.1 边界保护

测试评价方法如下。

- a) 测试方法:
- 1) 查验是否已在电子邮件系统外围部署防火墙,验证安全规则配置是否合理,如只允许必要的端口和协议通过、限制源 IP 地址等;
 - 2) 查验是否具备对邮件传输协议进行实时监测和分析的能力,发送使用非标准或异常邮件传输协议的邮件,验证是否能识别上述邮件并可采取阻断、记录或报警等操作。
- b) 预期结果:
- 1) 防火墙已部署并配置合理的安全规则;
 - 2) 具备对邮件传输协议进行实时监测和分析的能力,可将使用非标准或异常邮件传输协议的邮件采取阻断、记录或报警等操作。
- c) 结果判定:
- 1) 若上述 1)~2) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
 - 2) 若上述 1)~2) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.3.2 主机安全监测

测试评价方法如下。

- a) 测试方法:
- 1) 查验是否进行服务器硬件(如 CPU、内存、磁盘、网络等)及软件(如数据库、Web 服务、中间件等)运行状态监测,模拟硬件或软件故障,验证是否能及时发出报警;
 - 2) 查验是否能识别不符合协议规范的网络会话数据流并提取该会话所属进程的基本信息、远端 IP 地址,构造不符合协议规范的网络会话进行测试,验证是否能识别异常网络会话

数据流并提取该会话所属进程的基本信息(如进程名、进程 ID 等)和远端 IP 地址;

- 3) 查验开发方是否提供系统业务运行时命令执行、进程调用、文件使用等情况的相关文档,查验是否支持针对命令执行、进程调用、文件使用等行为的实时监测。

b) 预期结果:

- 1) 已进行服务器硬件及软件运行状态监测,能对服务器硬件或软件故障进行及时告警;
- 2) 可识别不符合协议规范的网络会话数据流,并准确提取出该会话所属进程基本信息和远端 IP 地址;
- 3) 开放方提供的相关文档包含命令执行、进程调用、文件使用等情况,支持对命令执行、进程调用、文件使用等进行实时监测。

c) 结果判定:

- 1) 若上述 1)~3)的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~3)的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.3.3 网络安全监测

测试评价方法如下。

a) 测试方法:

- 1) 查验是否配置专用的安全监测设备,部署方式、安全策略是否合理;
- 2) 查验开发方提供的相关文档,验证是否对邮件系统用户、邮件组织用户、邮件审计用户、邮件安全用户、邮件用户允许访问的 Web 业务路径及接口信息进行说明以及记录信息是否完整、明确;
- 3) 分别使用被测评单位邮件系统测试账户、非被测评单位邮件系统测试账户向测试账户发送包含异常编码(如乱码、非法字符等)的测试邮件,验证是否能识别上述邮件并进行记录及报警;
- 4) 分别使用被测评单位邮件系统测试账户、非被测评单位邮件系统测试账户向测试账户发送附件包含无法识别文件格式的测试邮件,验证是否能识别上述邮件并进行记录及报警;
- 5) 分别使用被测评单位邮件系统测试账户、非被测评单位邮件系统测试账户向测试账户发送包含木马程序的测试邮件,验证监测设备是否检测到木马植入攻击并及时进行报警;
- 6) 模拟隐蔽后门攻击行为,验证监测设备是否检测到隐蔽后门攻击并及时进行报警;
- 7) 模拟异常端口使用行为,验证监测设备是否检测到异常端口使用并及时进行报警;
- 8) 模拟邮件服务器网络异常通信行为,验证监测设备是否检测到邮件服务器网络异常通信行为并及时进行报警;
- 9) 通过邮件系统测试账户模拟异常接收邮件(如通过非常用登录 IP 地址下载大量邮件)和发送邮件(如对外发送垃圾邮件、钓鱼邮件以及包含敏感信息的邮件等)行为,验证监测设备是否检测到异常收发邮件行为;
- 10) 模拟在邮件服务器的 Web 页面上植入恶意代码,尝试访问相应 Web 网页,验证监测设备是否检测到邮件服务器 Web 网页挂马攻击行为并及时进行报警;
- 11) 模拟在邮件服务器的 Web 页面上添加隐藏或不可见的恶意链接,尝试访问相应 Web 网页,验证监测设备是否检测到邮件服务器 Web 网页隐藏、不可见链接攻击行为并及时进行报警;
- 12) 在邮件正文或附件中插入一组预定义的敏感关键词或语义含敏感信息的文字,尝试发送测试邮件,验证监测设备是否检测敏感信息外发并及时进行报警、阻断;

- 13) 若采用云计算环境,查验合同、安全管理规定、云计算环境安全能力资质等材料,验证云服务提供者是否对所提供的云服务进行持续风险监测,是否符合 GB/T 31168—2023 中的云服务的业务连续性要求。

b) 预期结果:

- 1) 专用安全监测设备以旁路接入方式部署在电子邮件系统出入口,安全策略配置合理,能正常接收和分析流量;
- 2) 开放方提供的相关文档包含邮件系统用户、邮件组织用户、邮件审计用户、邮件安全用户、邮件用户允许访问的 Web 业务路径及接口等情况,记录信息完整、明确;
- 3) 已对流转过程中的邮件是否符合编码标准进行监测,相关测试邮件均被记录及报警;
- 4) 已对流转过程中的邮件附件进行监测,相关测试邮件均被记录及报警;
- 5) 已进行木马植入攻击监测,相关测试邮件均被记录及报警;
- 6) 已进行隐蔽后门监测,相关隐蔽后门攻击行为均被记录及报警;
- 7) 已进行异常端口使用监测,相关异常端口使用行为均被记录及报警;
- 8) 已进行邮件服务器网络异常通信行为监测,相关邮件服务器网络异常通信行为均被记录及报警;
- 9) 已进行异常收发邮件行为监测,相关异常收发邮件行为均被记录及报警;
- 10) 已进行邮件服务器 Web 网页挂马攻击行为监测,相关邮件服务器 Web 网页挂马攻击行为均被记录及报警;
- 11) 已进行邮件服务器 Web 网页隐藏、不可见链接攻击行为监测,相关邮件服务器 Web 网页隐藏、不可见链接攻击行为均被记录及报警;
- 12) 监测设备支持通过关键词和语义识别防止敏感信息外发,测试邮件被系统拦截,并提示含有敏感信息;
- 13) 若采用云计算环境,云服务提供者对所提供的云服务进行持续风险监测,并根据 GB/T 31168—2023 要求保证云服务的业务连续性。

c) 结果判定:

- 1) 若上述 1)~13) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~13) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.3.4 反垃圾邮件

测试评价方法如下。

a) 测试方法:

- 1) 按照 GB/T 30282—2023 中测试评价方法进行测试;
- 2) 查验是否支持对来自本单位内部邮件账户发送的垃圾邮件的检测、拦截,使用被测评单位邮件测试账户分别向该单位及其他单位邮件测试账户发送垃圾邮件,验证上述测试邮件是否被检测、拦截。

b) 预期结果:

- 1) 符合 GB/T 30282—2023 中相关预期结果;
- 2) 支持对来自本单位内部邮件账户发送的垃圾邮件的检测、拦截,相关测试邮件均被检测、拦截。

c) 结果判定:

- 1) 若上述 1)~2) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要

求,否则判定为不符合;

- 2) 若上述 1)~2)的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.3.5 防病毒

测试评价方法如下。

a) 测试方法:

- 1) 查验是否具备两种以上的防病毒引擎且至少包含一种启发式防病毒引擎,使用近一年典型病毒样本分别对每种防病毒引擎进行测试,验证病毒检测效果;
- 2) 创建用于检测特定恶意程序或行为的自定义规则,使用包含特定恶意程序或行为的样本进行测试,验证是否能根据自定义规则进行识别并处理;
- 3) 分别构造邮件正文、邮件附件中包含有效病毒文件的恶意邮件并发送至邮件系统测试账户,验证是否能检测出恶意邮件中的病毒并过滤;
- 4) 查验是否支持在线升级与离线升级病毒库,分别对病毒库进行在线升级与离线升级,验证病毒库是否均能升级至最新版本;
- 5) 使用被测评单位邮件系统测试账户分别向该单位及其他单位邮件测试账户发送存在恶意病毒的邮件,验证上述测试邮件是否被检测、拦截;
- 6) 配置系统安全策略以执行不同的病毒处理操作(如拒绝发送、拒绝接收、添加警告信息等),使用被测评单位邮件系统测试账户分别向该单位及其他单位邮件系统测试账户发送存在病毒的测试邮件,使用非被测评单位邮件系统测试账户向该单位邮件系统测试账户发送存在病毒的测试邮件,验证系统是否能根据配置的策略对邮件进行相应处理;
- 7) 配置符合 GB/T 44886.4—2026 要求的威胁信息,如恶意样本哈希值、恶意样本检测规则等,发送包含相关恶意样本的测试邮件,验证邮件系统是否能根据接收到的威胁信息对邮件进行病毒识别。

b) 预期结果:

- 1) 具备两种以上的防病毒引擎且至少包含一种启发式防病毒引擎,能识别并清除已知病毒样本,启发式防病毒引擎具备对未知病毒样本的检测能力;
- 2) 支持自定义规则查杀特定恶意程序,能对包含该恶意程序特征或行为的样本进行识别及处理;
- 3) 能对邮件正文、邮件附件中包含的病毒进行过滤,能分别对邮件正文及附件中携带病毒的测试样本进行识别及处理;
- 4) 支持在线升级与离线升级病毒库,通过两种方式均能将病毒库升级至最新版本;
- 5) 支持对来自本单位内部邮件账户发送的存在恶意病毒的邮件的检测、拦截,相关测试邮件均被检测、拦截;
- 6) 对存在病毒的邮件可设置拒绝发送或拒绝接收、在邮件中添加警告信息、不处理等操作,相关测试邮件处理结果与预期一致;
- 7) 支持 GB/T 44886.4—2026 共享威胁信息,相关测试邮件均被准确识别并告警。

c) 结果判定:

- 1) 若上述 1)~7)的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~7)的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.3.6 防钓鱼

测试评价方法如下。

a) 测试方法：

- 1) 准备发件人邮件域、正文或附件中包含不同域名、URL 链接的邮件样本,包括正常邮件和有害邮件,分别使用被测评单位及非被测评单位邮件系统测试账户发送上述邮件至测试账户,验证系统是否能正确识别出有害邮件;
- 2) 准备邮件主题、正文或附件中包含不同关键词和语义的邮件样本,包括正常邮件和有害邮件,分别使用被测评单位及非被测评单位邮件系统测试账户发送上述邮件至测试账户,验证系统是否能正确识别出有害邮件;
- 3) 准备邮件正文中包含外部网站的 URL 链接、短地址链接和图形二维码的样本邮件,发送上述邮件至邮件系统测试账户,验证邮件系统是否在用户打开前发出风险提示;
- 4) 准备邮件附件中包含嵌入外部网站的 URL 链接、短地址链接和图形二维码的样本邮件,发送上述邮件至邮件系统测试账户,验证邮件系统是否在用户下载附件前发出风险提示;
- 5) 配置黑名单域名、URL 链接,准备正文、附件中包含黑名单地址的邮件样本,分别使用被测评单位及非被测评单位邮件系统测试账户发送上述邮件至测试账户,验证邮件系统是否对黑名单地址进行阻断;
- 6) 使用被测评单位邮件系统测试账户分别向该单位及其他单位邮件系统测试账户发送钓鱼邮件,验证上述测试邮件是否被检测、拦截。
- 7) 配置符合 GB/T 44886.4—2026 要求的威胁信息,如发件人邮箱账户、附件文件哈希值、邮件主题及正文等,发送涉及威胁信息的测试邮件,验证邮件系统是否能根据接收到的威胁信息对邮件进行识别并告警;
- 8) 准备邮件正文及附件中包含不同 URL 链接、短地址链接和图形二维码的邮件样本,包括正常邮件和有害邮件,分别使用被测评单位及非被测评单位邮件系统测试账户发送上述邮件至测试账户,验证系统是否能对相关链接和图形二维码指向的页面进行安全检测并正确识别出有害邮件。

b) 预期结果：

- 1) 对于发件人邮件域、正文或附件中包含不同域名、URL 链接的邮件样本,系统能准确地将有害邮件进行标记,误报率及漏报率符合要求;
- 2) 对于邮件主题、正文或附件中包含不同关键词和语义的邮件样本,系统能准确地将有害邮件进行标记,误报率及漏报率符合要求;
- 3) 对于邮件正文中指向外部网站的 URL 链接、短地址链接和图形二维码,用户点击打开相关测试邮件前,均发出风险提示;
- 4) 对于邮件附件嵌入外部网站的 URL 链接、短地址链接和图形二维码,用户下载相关测试邮件附件前,均发出风险提示;
- 5) 支持设置域名、URL 链接黑名单,对于正文或附件中包含黑名单域名、URL 链接的邮件样本,系统能准确阻断;
- 6) 支持对来自本单位内部邮件账户发送的钓鱼邮件的检测、拦截,相关测试邮件均被检测、拦截;
- 7) 支持 GB/T 44886.4—2026 共享威胁信息,相关测试邮件均被准确识别并告警;
- 8) 对于邮件正文及附件中包含不同 URL 链接、短地址链接和图形二维码的邮件样本,系统能对相关链接和图形二维码指向的页面进行安全检测并准确地将有害邮件进行标记,误报率及漏报率符合要求。

c) 结果判定：

- 1) 若上述 1)~7) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合；
- 2) 若上述 1)~8) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.3.7 安全审计

8.3.7.1 数据库操作审计

测试评价方法如下。

a) 测试方法：

- 1) 使用不同权限的用户执行多种 SQL 操作,验证日志记录是否包括时间、数据库服务器名称、IP 地址、MAC 地址、端口号、用户名、操作执行结果及原始 SQL 语句,是否具备日志审计功能；
- 2) 使用不同权限的用户执行多种 SQL 操作,包括异常请求行为和数据库敏感信息查询行为,验证是否具备双向审计功能,异常请求及数据库返回敏感信息行为是否均被记录并审计；
- 3) 配置多种自定义审计策略,策略元素涉及时间、来源、角色、SQL 操作类型、事件类型、数据库 SQL 语句关键字、延迟时间、影响行数、异常串、基于数据库服务器组或者资产组等,验证系统是否能根据配置的策略正确地记录或过滤审计日志；
- 4) 以数据库访问时间、IP 地址、端口号、用户名、操作类型、SQL 中的关键词等条件进行组合查询,验证检索结果的准确性和完整性；
- 5) 模拟 SQL 注入、已知数据库漏洞、口令猜解、缓冲区溢出等攻击行为,验证是否能根据预设的安全规则库进行识别并报警；
- 6) 模拟最高权限滥用、误操作、恶意操作等行为,验证相关行为是否被识别并报警。

b) 预期结果：

- 1) 支持记录和审计数据库 SQL 级操作,日志记录完整；
- 2) 具备双向审计功能,异常请求及数据库返回敏感信息行为均被记录并审计；
- 3) 能定义审计策略,并根据配置的策略正确地记录或过滤审计日志；
- 4) 具备丰富的数据查询检索功能,基于数据库访问时间、IP 地址、端口号、用户名、操作类型、SQL 中的关键词等条件进行查询时均能获取准确结果；
- 5) 具备数据库防攻击安全规则库,能根据预设置策略发现诸如 SQL 注入、已知数据库漏洞、口令猜解、缓冲区溢出等异常行为,相关测试行为能被识别并报警,误报率及漏报率符合要求；
- 6) 具备权限预警功能,能针对最高权限滥用、误操作、恶意操作等行为进行报警和定位。

c) 结果判定：

- 1) 若上述 1)~6) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合；
- 2) 若上述 1)~6) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.3.7.2 日志审计

测试评价方法如下。

a) 测试方法:

- 1) 查验是否具备操作系统安全日志,日志记录信息要素是否完整,是否定期进行审计;
- 2) 查验是否具备 Web 中间件安全日志,日志记录信息要素是否完整,是否定期进行审计;
- 3) 查验是否具备邮件系统接口调用过程操作日志,日志记录信息要素是否完整,是否定期进行审计;
- 4) 查验是否具备邮件应用系统日志,日志记录信息要素是否完整,是否定期进行审计;
- 5) 按照 8.2.2.3 中的测试方法进行测试,查验是否实现数据库访问日志记录功能,是否定期进行审计;
- 6) 查验是否具备数据加密设备安全日志,日志记录信息要素是否完整,是否定期进行审计;
- 7) 查验是否对审计记录进行保护并定期进行备份。

b) 预期结果:

- 1) 具备操作系统安全日志,日志记录信息要素完整,定期进行审计;
- 2) 具备 Web 中间件安全日志,日志记录信息要素完整,定期进行审计;
- 3) 具备邮件系统接口调用过程操作日志,日志记录信息要素完整,定期进行审计;
- 4) 具备邮件应用系统日志,日志记录信息要素完整,定期进行审计;
- 5) 预期结果与 8.2.2.3 预期结果一致;
- 6) 具备数据加密设备安全日志,日志记录信息要素完整,定期进行审计;
- 7) 已对审计记录进行保护并定期备份,可避免受到未预期的删除、修改或覆盖等。

c) 结果判定:

- 1) 若上述 1)~7) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~7) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.3.8 防漏洞

测试评价方法如下。

a) 测试方法:

- 1) 查验系统管理员是否使用默认口令和默认系统配置,尝试将系统管理员口令、系统配置修改为默认配置,验证系统是否强制要求修改;
- 2) 通过专业漏洞扫描工具、安全检测技术、人工代码审计、渗透测试等方式对邮件系统进行检测,验证邮件系统各组件、接口、功能模块等是否存在安全漏洞;
- 3) 查验邮件系统中是否采用第三方厂商部件,若采用,则要求第三方厂商提供部件信息(名称、版本号、功能描述等)以及产品安全报告和安全评估资料,同时对部件进行安全测试,验证第三方厂商部件是否存在漏洞。

b) 预期结果:

- 1) 默认口令无法直接登录,或首次登录时系统立即提示修改默认口令和系统配置,且修改时系统提供符合安全标准的口令复杂度和合理配置选项;
- 2) 未发现已知安全漏洞,系统在各检测场景下正常运行,无数据泄露、崩溃等问题;
- 3) 未采用第三方厂商部件,或采用第三方厂商部件,相关部件不存在安全漏洞。

c) 结果判定:

- 1) 若上述 1)~3) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要

求,否则判定为不符合;

- 2) 若上述 1)~3)的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.3.9 日常维护

测试评价方法如下。

a) 测试方法:

- 1) 查验是否存在配套运维管理制度,查看相关运维管理材料,验证相关管理制度是否完善;
- 2) 查验邮件系统运行状态检查记录,验证系统管理员是否定期检查和记录电子邮件系统运行状态,异常情况是否及时按要求上报;
- 3) 查验系统审计日志,验证管理员是否定期修改口令,修改频率是否符合安全管理要求;
- 4) 查验漏洞检测、系统升级和加固记录表,并抽取部分系统升级和加固记录进行实机对比,验证管理员是否定期对电子邮件系统进行漏洞检测、升级和加固;
- 5) 查验电子邮件系统故障处理流程、维护记录,并与运维工作流程进行对比,验证是否按运维工作流程进行维护并记录维护操作内容;
- 6) 查验变更电子邮件系统配置操作是否合规,查阅维护记录,并与运维工作流程进行对比,验证是否按运维工作流程进行配置变更并记录了配置变更内容;
- 7) 查验电子邮件系统移动存储介质使用情况,查阅系统日志,查找是否有与移动存储介质相关的异常活动,验证是否有明确的安全策略禁止在电子邮件系统中使用移动存储介质;
- 8) 若采用云计算环境,查验是否符合下列要求:
 - 查验运维审计记录,验证系统管理员是否按运维工作流程对云上业务系统进行运维审计;
 - 查验云服务提供者相关证明材料,验证是否提供迁移与退出时的存储、销毁、删除计划;
 - 查验相关证明材料,验证是否做好云内的安全策略配置和更新、云产品账号管理、访问授权、权限管理等。

b) 预期结果:

- 1) 存在配套运维管理制度,管理制度中明确规定对电子邮件系统的运维要求;
- 2) 系统管理员定期检查电子邮件系统运行状态并记录,维护记录完整,异常情况按要求上报;
- 3) 系统管理员定期修改电子邮件系统管理员口令,修改频率符合安全管理要求;
- 4) 系统管理员定期对电子邮件系统进行漏洞检测、升级和加固,相关记录完整,抽取记录与系统实际情况符合;
- 5) 电子邮件系统发生故障时,按照运维工作流程进行维护并记录维护操作内容,维护记录内容符合运维工作流程相关规定;
- 6) 变更电子邮件系统配置时,按照运维工作流程进行操作并记录配置变更内容,维护记录内容符合运维工作流程相关规定;
- 7) 未在电子邮件系统(邮件客户端除外)中使用移动存储介质,有明确的安全策略禁止在电子邮件系统中使用移动存储介质;
- 8) 若采用云计算环境,符合下列要求:
 - 系统管理员按运维工作流程对云上业务系统进行运维审计,确保云服务的安全性、稳定性;
 - 迁移与退出时,云服务提供者提供详细的存储、销毁、删除计划,能有效擦除数据;

——已做好云内的安全策略配置和更新、云产品账号管理、访问授权、权限管理等。

c) 结果判定：

- 1) 若上述 1)~8) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~8) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

8.3.10 基础设施

测试评价方法如下。

a) 测试方法：

- 1) 查验邮件服务提供者相关证明文件,查验邮件服务器的服务域名解析 IP 及邮件交换记录(MX 记录)与邮件服务提供者给出的相关材料是否一致,验证邮件服务器基础设施是否位于中国境内;
- 2) 若采用云计算环境,查验云服务提供者相关证明材料,验证邮件系统是否部署于低于其网络安全保护等级的云计算环境。

b) 预期结果：

- 1) 邮件服务器基础设施位于中国境内,邮件服务提供者能提供邮件服务器基础设施位于中国境内的相关证明文件,服务域名解析 IP 及邮件交换记录(MX 记录)与邮件服务提供者给出的相关材料一致;
- 2) 若采用云计算环境,邮件系统未部署于低于其网络安全保护等级的云计算环境。

c) 结果判定：

- 1) 若上述 1)~2) 的实际测试结果与对应的预期结果均一致,则判定为符合基本级安全要求,否则判定为不符合;
- 2) 若上述 1)~2) 的实际测试结果与对应的预期结果均一致,则判定为符合增强级安全要求,否则判定为不符合。

附 录 A
(资料性)

电子邮件系统安全级别选择方法

本文件中,电子邮件系统的安全要求按其保障强度可划分为基本级和增强级两个等级的安全要求。各单位可根据本单位属性、用户数量和业务重要度选择使用基本级或增强级技术要求,当相关单位的电子邮件系统符合任意一条参考选择指标要求时,使用增强级安全要求。电子邮件系统安全级别选择方法见表 A.1。

表 A.1 电子邮件系统安全级别选择方法

级别选择因素	参考选择指标		技术安全要求级别
单位属性	部委或省级邮箱系统、国有及中央企业、重要研究机构	是	增强级安全要求
		否	基本级安全要求
注册用户数	累计用户总数≥50 万	是	增强级安全要求
		否	基本级安全要求
业务重要度	如发生泄密事件后会对社会秩序或公共利益严重损害,或者对国家安全造成损害;或按照 GB/T 22240—2020 安全保护等级要求中定级为三级以上(含三级)的邮件系统	是	增强级安全要求
		否	基本级安全要求

附录 B
(资料性)

基于加密技术的电子邮件系统模型

基于加密技术的电子邮件系统模型见图 B.1。

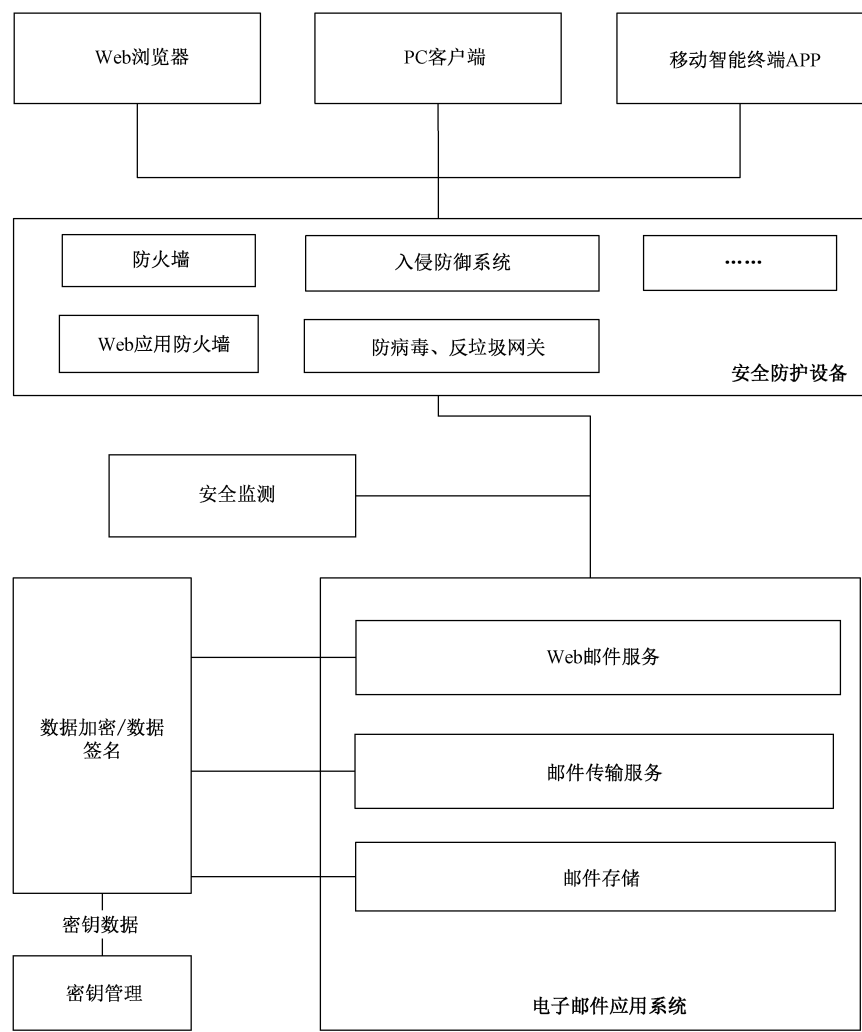


图 B.1 基于加密技术的电子邮件系统模型

参 考 文 献

- [1] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
-

