ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36618—2018

信息安全技术　金融信息服务安全规范

Information security technology—Specification for financial information service security

2018-09-17 发布　　2019-04-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:北京济安金信科技有限公司、中国人民大学、中国科学院信息工程研究所、清华大学五道口金融学院、中国经济信息社、万得信息技术股份有限公司、东方财富信息股份有限公司、上海大智慧股份有限公司、腾讯科技(北京)有限公司。

本标准主要起草人:杨健、荆继武、洪彬、陈峰、王铁牛、秦文怡、钱明辉、王克平、朱祥文、王胜先、马立、雷雨、刘子航、陈楠、李尚昊、贺裴菲、周立、王正位、李秀明、覃继胜、巨峰、范小莉、程鸿岩、徐可、冯卫强、吴征、张瑾、王雯雯。

引　言

金融信息对于国家金融政策制定者、金融机构以及投资决策者具有特别重要的意义。

金融信息安全是国家信息安全的组成部分，信息资源、信息系统和信息网络等存在的安全问题不仅影响金融信息服务活动，而且可能影响国家金融安全，为了提高金融信息质量、提升金融信息服务水平、维护市场健康发展、保障用户权益，因此特制定本标准。

本标准对金融信息服务提供商的内部管理及安全技术等方面提出了基本要求，标准的制定将有利于金融信息服务提供商规范金融信息服务过程，防范金融信息服务安全风险，不断提高金融信息服务质量。

信息安全技术　金融信息服务安全规范

1　范围

本标准规定了金融信息服务提供商提供金融信息服务时的基本原则、服务过程要求、技术要求和管理要求。

本标准适用于在中华人民共和国境内注册或登记的国内外金融信息服务提供商提供金融信息服务的活动。

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 20271—2006　信息安全技术　信息系统通用安全技术要求

GB/T 20272—2006　信息安全技术　操作系统安全技术要求

GB/T 20988—2007　信息安全技术　信息系统灾难恢复规范

GB/T 21028—2007　信息安全技术　服务器安全技术要求

GB/T 28827.1—2012　信息技术服务　运行维护　第1部分：通用要求

GB/T 28827.3—2012　信息技术服务　运行维护　第3部分：应急响应规范

GB/T 31500—2015　信息安全技术　存储介质数据恢复服务要求

GB/T 32924—2016　信息安全技术　网络安全预警指南

GB/T 33132—2016　信息安全技术　信息安全风险处理实施指南

GB/T 33530—2017　人力资源外包服务规范

GB/T 33770.1—2017　信息技术服务　外包　第1部分：服务提供方通用要求

3　术语和定义

下列术语和定义适用于本文件。

3.1

金融信息　financial information

反映金融活动状态及其变化的实质内容的信息。

注：包括与金融活动和金融市场相关的各种信号、指令、数据、消息和报告等。

3.2

金融信息服务　financial information service

向从事分析、决策、交易、清算等金融行业以及相关机构和个人，提供可能影响金融活动和金融市场的信息、数据、软件以及相关信息技术等方面的活动。

3.3

金融信息服务提供商　financial information services provider

提供金融信息服务的组织。

4 基本原则

4.1 准确性

准确性是信息和数据与真实情况的接近程度。金融信息服务提供商应保证提供金融信息真实、准确，信息的表述不会引起歧义，能够反映信息的真实状态，不得有虚假记载或误导性陈述。

4.2 完整性

完整性是信息在存储和传输的过程中，不被非法授权修改、破坏、插入、延迟、乱序和丢失的特性。金融信息服务提供商对金融信息进行采集、加工、处理和提供时应保证信息完整，没有重大遗漏或信息歪曲失真的情况发生。

4.3 可用性

可用性是授权实体在需要时可有效访问和可利用的属性。金融信息服务提供商应保证提供金融信息服务的网络、信息系统随时可用，使合法授权的用户可以及时获取所需的金融信息。

4.4 时效性

时效性是信息仅在一定时间段内对决策具有价值的属性。金融信息服务提供商应保证金融信息及时提供和更新。针对不同级别用户可以划分优先等级。

4.5 可信性

可信性是提供确实可信任服务的属性。金融信息服务提供商应保证所提供的金融信息来源明确，金融信息加工处理经过审核确认。

4.6 合规性

合规性是符合并遵守法律、政策、规章、程序及合同的能力。金融信息服务提供商在采集、加工、处理和提供信息时不应违反知识产权、著作权等法律法规要求。

4.7 抗抵赖性

抗抵赖性是一个活动或事件已经发生，且不可否认的能力。金融信息服务提供商应通过技术措施保证所提供的金融信息服务具备抗抵赖性，并可以追溯金融信息的相关信息。

4.8 保密性

保密性是信息对未授权的个人、实体或过程不可用或不可泄漏的特性。金融信息服务提供商应通过完备的信息安全体系，保证未授权者无法使用信息，在信息使用和传输过程中不会被非法泄漏而扩散。

4.9 可控性

可控性是信息的传播及内容具有控制能力的特性。金融信息服务提供商应掌握、控制信息的流向和使用范围等，以便国家相关监管部门审查。包括但不限于：可控性，授权机关可以随时控制信息的机密性；访问可控性，每一个用户只能访问自己被授权可以访问的信息；等级可控性，系统中可利用的信息及资源应当划分保密等级。

5 服务过程要求

5.1 概述

金融信息服务提供商在提供金融信息服务时，基本服务过程包括信息采集、加工与处理及提供信息3个过程。

5.2 金融信息采集

5.2.1 金融信息来源

金融信息服务提供商应对信息来源进行必要的说明，包括但不限于以下3个方面：

a) 信息的来源，包括但不限于购买第三方数据库、交叉授权获取、网络采集和信息服务过程产生等；
b) 信息的形式，包括但不限于数据、文本、文件、图片、音频和视频等；
c) 信息的传输方式，包括但不限于有线通讯传输、无线通讯传输和数字通讯传输等方式。

5.2.2 金融信息采集基本要求

金融信息服务提供商在进行金融信息采集时，采集要求包括但不限于以下4项：

a) 金融信息服务提供商应设置专人负责信息生产者和提供者的资质审核；
b) 金融信息服务提供商应明确金融信息来源、采集方式、采集范围等内容，并记录存档；
c) 制定标准的采集模板、数据采集方法、策略和规范，采集策略参数配置应包含采集周期、有效性检测时间、入口地址和采集深度等；
d) 对初次采集的金融信息，应采用人工与技术相结合的方式根据其来源、类型或重要程度进行分类。

5.2.3 金融信息采集方式

5.2.3.1 公开方式

金融信息服务提供商应通过多种渠道采集已被合法公开披露的金融信息。

5.2.3.2 约定方式

金融信息服务提供商应通过与有关机构或个人约定的方式采集金融信息，包括但不限于授权引用、采购等。

5.2.3.3 其他方式

金融信息服务提供商通过除5.2.3.1和5.2.3.2以外的其他方式采集金融信息时，应采用符合金融监管要求的方式。

5.3 金融信息加工与处理

5.3.1 加工与处理基本要求

金融信息服务提供商在金融信息加工与处理过程中，应包括但不限于以下两项要求：

a) 加工和处理的金融信息应通过审查复核；
b) 加工与处理过程中应符合信息的准确性和完整性原则。

5.3.2 加工与处理方法

金融信息服务提供商应详细说明金融信息从收集、加工以及到录入的过程中所采用的方法、设备、工具软件以及所采用的数据质量控制规范，包括但不限于以下 3 个方面：

a) 使用有合法授权的软件、设备、工具进行数据采集、加工处理和发布；
b) 保证所采用的软件系统、硬件系统持续稳定运行，保证金融信息存储、金融信息传输、金融信息使用等过程安全可靠；
c) 在金融信息加工处理过程中，保证数据信息不被非法授权查看、复制和篡改。

5.4 金融信息提供

5.4.1 金融信息提供基本要求

金融信息服务提供商对外提供金融信息的基本要求应包括但不限于以下 4 项：

a) 在其网站主页的显著位置标明其经营许可证编号或者备案号；
b) 通过合法合规的程序、渠道为客户提供金融信息服务，同时记录金融信息的内容、发布时间、互联网地址或域名等信息，转载的金融信息应注明信息来源及转载时间；
c) 明确客户使用金融信息的范围并提供免责声明条款；
d) 在金融信息传输质量和速度受到影响时，及时通知客户受影响数据范围和时间区间。

5.4.2 提供方式

金融信息服务提供商对外提供金融信息的方式包括但不限于通过书面文件、电子邮件、网络媒介等可靠与可确认的方式提供金融信息。

6 技术要求

6.1 基础设施安全

金融信息基础设施包括提供金融信息服务所使用的硬件设备和软件设备，包含主机、服务器、存储设备和网络设备等硬件设备；操作系统、数据库管理系统和应用软件等软件设备。金融信息基础设施在网络安全方面，应符合国家网络安全相关规定，包括但不限于以下 7 个方面：

a) 金融信息服务提供商应采购经过认证合格或安全检测合格的网络关键设备和网络安全专用产品；
b) 金融信息服务提供商应采取措施保障主机、服务器和存储等硬件设备的安全，其中，对服务器的安全要求至少应符合 GB/T 21028—2007 中 5.2 的规定；
c) 提供金融信息服务的信息系统的通用安全要求至少应符合 GB/T 20271—2006 中 6.2 的规定，其中对操作系统的安全要求至少应符合 GB/T 20272—2006 中 4.2 的规定；
d) 金融信息服务提供商应建立完善的网络安全设施和安全管理方案，建立及时更新的防病毒系统，保护系统和数据库的安全；
e) 金融信息服务提供商应采用不同方法检测网络、主机和存储设备等不同层面的基础设施，最后进行总体安全检测工作，并对涉及个人信息、保密信息等的安全风险进行抽查检测；
f) 检测金融信息和数据在采集、加工、处理、存储、传输和使用过程中完整性是否受到破坏，并在检测到完整性错误时采取必要的恢复措施；
g) 金融信息服务提供商的机房选址应遵守国家有关规定。

6.2 软件安全

金融信息服务提供商应制定一套完整的软件安全解决方案，软件安全应包括但不限于以下 4 个方面：

a) 在服务器端对系统软件、应用软件及其配置进行定期备份，并做好相应的记录；
b) 及时掌握系统及应用软件公布的软件漏洞，并进行更新修正；
c) 对所有的系统软件、应用软件操作执行审计日志，并定期对日志进行分析，发现问题及时处理；
d) 软件发布或更新版本前，应进行安全检测。

6.3 网络安全

金融信息服务提供商应具备网络安全保护能力，包括但不限于以下 5 个方面：

a) 端口扫描、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网络攻击的防护；
b) 采取系统访问控制、数据保护、监测、记录网络运行状态、网络安全事件的技术措施；
c) 金融信息服务提供商应指定专人对上网的金融信息进行保密检查；
d) 涉及国家安全、商业秘密的信息设备，应严格控制互联网接入口数量和接入终端数量；
e) 按 GB/T 32924—2016 中第 4 章的规定，确定金融信息服务系统的网络安全重要程度，具备预警响应及处置的能力。

6.4 数据安全

6.4.1 提供商数据安全要求

金融信息服务提供商对金融信息服务相关的数据安全基本要求至少应符合 GB/T 20271—2006 中 6.2.3 的规定，同时应制定完整的数据安全解决方案，包括但不限于以下 5 个方面：

a) 应提供数据资料的分类存储、恢复、调用、加密和销毁等技术措施；
b) 检测金融信息和数据在采集、加工、处理、存储、传输和使用过程中完整性，并在检测到完整性错误时采取必要的恢复措施；
c) 提供本地数据备份与恢复功能，采用实时备份与异步备份或增量备份与完全备份的方式，确定数据备份的范围、时间间隔等内容；
d) 数据在存储介质上的数据恢复服务应符合 GB/T 31500—2015 中第 6 章的规定；
e) 具备数据安全传输解决方案，以安全的网络、会话管理和恢复特性等来确保数据安全和数据传输安全。

6.4.2 用户数据安全要求

金融信息服务提供商应严格保管用户数据，遵循个人信息保护相关的法律法规，用户数据安全要求包括但不限于以下 6 项：

a) 制定用户数据管理制度，明确各岗位在用户数据保护管理方面的工作内容，对用户数据的访问、存储、使用、传输和销毁等环节提出具体要求；
b) 严格管理、控制对用户数据的访问权限，监控所有用户数据的访问活动；
c) 使用用户数据时，包括身份信息、认证信息和衍生信息等，不得用于商业目的，保证其不被非法泄漏；向境外提供用户数据时，应根据相关法规要求，完成安全评估后使用；
d) 应告知用户用途及范围，用户许可后才允许使用数据；
e) 及时处理涉及用户数据的突发安全事件；

f) 检查、监督用户数据管理制度的落实。

6.5 运行安全

金融信息服务提供商应制定并依据运维制度开展日常工作，内容包括总体安全策略、安全技术框架、安全管理策略、机房管理制度、系统维护制度、安全需求分析和详细设计方案等。

金融信息服务提供商应按 GB/T 28827.1—2012 中第 4 章的规定，从人员、资源、技术和过程 4 个方面确保运行安全的工作。同时，金融信息服务提供商应采用技术措施对系统和应用软件的行为及内容进行监测和记录，监测到非法操作或非法信息时，应及时作出响应处理工作；提供对客体身份、用户身份、主体身份、主机身份和安全事件的审计，审计记录应包括事件日期、事件、类型和描述等信息，保护审计记录，避免受到未预期的删除、修改或覆盖等。

金融信息服务提供商处理系统应急响应工作时应符合 GB/T 28827.3—2012 中第 7 章、第 8 章的规定。

6.6 容灾和恢复

金融信息服务提供商应制定符合 GB/T 20988—2007 中第 7 章规定的容灾恢复方案，对容灾备份的工具、方式、频度、存储介质、保存期等进行规范。包括但不限于以下 4 个方面：

a) 根据数据的重要性，制定数据的容灾备份策略和恢复策略，备份策略应指明容灾备份数据的放置场所、文件命名规则、介质替换频率等内容；
b) 定期对容灾备份数据有效性进行检查，备份数据应异地保存；
c) 建立控制容灾数据备份和恢复过程的程序，定期进行数据灾备、恢复切换演练；
d) 对支撑灾难恢复系统运行的服务器、存储、安全、数据库进行实时监控。

7 管理要求

7.1 制度保障

金融信息服务提供商应制定完善的信息安全管理制度，信息安全管理制度的内容应包括但不限于以下 4 个方面：

a) 信息安全管理的总体目标和指导原则；
b) 信息安全管理的定义、范围，应符合国家标准、行业标准和组织制度的规定；
c) 信息安全管理的一般责任和具体责任；
d) 违反信息安全管理制度的惩罚原则和具体措施。

7.2 管理职责

金融信息服务提供商应建立独立的部门，落实信息安全管理相关职责，包括但不限于以下 3 个方面：

a) 主负责人应作为信息安全管理第一责任人，同时指定信息安全管理日常工作的分管负责人；
b) 对从事信息安全管理工作的相关负责人的安全背景进行审核；
c) 设立层级清晰、权责明确的管理团队，确定团队人员职责，负责具体信息安全管理实施工作，其职责主要包括：研究和执行国家和行业有关信息安全的政策、法律和法规；制定和推广信息安全管理总体策略、管理规范和技术标准；定期审计信息安全管理措施；定期检查信息安全管理工作内容等。

7.3 人员管理

金融信息服务提供商应配备专职专岗人员负责对应的工作内容，且具备一定资质，遵循相关规定。包括但不限于以下4项要求：

a) 依据相关法律法规规定，配备专职专岗的系统管理员、网络管理员、安全审计员、安全保密管理员等核心信息安全相关岗位安全技术保障人员；
b) 确保安全技术保障人员数量满足金融信息安全服务工作需求；
c) 对信息安全服务岗位的人员建立人员档案，档案内容应包含人员基本信息、技术资格证明文件和参与信息安全服务的历史记录；
d) 工作人员应与提供商签订保密协议。

7.4 培训教育

金融信息服务提供商应做好工作人员的培训教育工作，包括但不限于以下两个方面：

a) 工作人员应定期接受安全管理相关培训，了解安全制度、安全要求、法律责任和安全处理程序等方面内容，并定期检查工作人员的掌握情况；
b) 工作人员应具备相关基础业务技能，新入职的工作人员需要接受一定的专业培训并通过考核才能从事相关的工作。

7.5 风险管理

金融信息提供商应依据有关信息安全管理制度、标准和规范，同时按GB/T 33132—2016第5章～第7章的规定，对其面临的信息安全风险进行管理。包括但不限于以下5项：

a) 制定风险管理方案，明确风险管理的目标、范围、人员、方法、评估方法、评估结果的形式等；
b) 通过风险识别，识别信息安全管理风险来源，并确定其影响区域、事件以及原因；
c) 通过风险分析，分析安全管理风险特性，确定其所带来的正面和负面的后果及这些后果发生的可能性；
d) 通过风险评价，依据风险分析的结果确定需要处理的风险和处理实施优先的决策；
e) 通过风险处理，确定风险的处理方案并对方案进行实施。

7.6 外包管理

金融信息服务提供商不应将第5章要求的服务外包，但信息技术咨询、基础环境集成实施和软件运维等服务可采用外包方式。金融信息服务提供商采购外包服务时，按GB/T 33770.1—2017第6章～第8章的规定。包括但不限于以下4项：

a) 制定服务外包信息安全管理策略和安全管理制度，确定外包服务商选择、安全管理程序、角色操作、评估及风险管理等制度、策略；
b) 指定本单位的外包服务负责人，监督、管理外包服务的质量，保证外包服务商的服务质量和服务标准；
c) 通过合同、协议或其他附件，明确外包单位在服务过程中使用和处理数据的所有权、使用边界等安全要求；
d) 采购人力资源外包服务时，按GB/T 33530—2017第3章～第9章的规定，进行管理、评估服务内容。

参 考 文 献

[1] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南
[2] GB/T 22118—2008 企业信用信息采集、处理和提供规范
[3] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求
[4] GB/T 27910—2011 金融服务 信息安全指南
[5] GB/T 29264—2012 信息技术服务 分类与代码
[6] GB/T 29765—2013 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
[7] GB/T 31168—2014 信息安全技术 云计算服务安全能力要求
[8] GB/T 32914—2016 信息安全技术 信息安全服务提供方管理要求
[9] JR/T 0071—2012 金融行业信息系统信息安全等级保护实施指引
[10] JR/T 0098.8—2012 中国金融移动支付 检测规范 第8部分:个人信息保护
[11] ISO/IEC 27033-1 Information technology—Security techniques—Network security—Part 1: Overview and concepts
[12] 服务贸易总协定(GATS),1995
[13] 计算机信息网络国际联网安全保护管理办法,1997
[14] 互联网信息服务管理办法,2000
[15] 外国机构在中国境内提供金融信息服务管理规定,2009
[16] 新闻记者证管理办法,2009
[17] 中华人民共和国网络安全法,2016
[18] 互联网新闻信息服务管理规定,2016