



中华人民共和国国家标准

GB/T 34080.2—2017

基于云计算的电子政务公共平台安全规范 第2部分：信息资源安全

Security specification of electronic government common platform based on
cloud computing—Part 2: Information resources security

2017-07-31 发布

2017-11-01 实施

中华人民共和国国家质量监督检验检疫总局 发布
中国国家标准化管理委员会

目 次

前言 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语、定义和缩略语..... 1

4 电子政务公共平台信息资源范畴 2

5 电子政务公共平台信息资源安全保护分类 2

6 电子政务公共平台信息资源安全保护要求 2

 6.1 第 1 类 2

 6.2 第 2 类 5

 6.3 第 3 类 6

 6.4 第 4 类 7

7 电子政务公共平台信息资源安全管理技术要求 7

 7.1 日常监测要求 7

 7.2 安全审计要求 8

 7.3 定位溯源要求 8

 7.4 日志留存要求 9

 7.5 应急处置要求 9

 7.6 安全风险评估要求 9

前 言

GB/T 34080《基于云计算的电子政务公共平台安全规范》分为 4 个部分：

- 第 1 部分：总体要求；
- 第 2 部分：信息资源安全；
- 第 3 部分：服务安全；
- 第 4 部分：应用安全。

本部分为 GB/T 34080 的第 2 部分。

本部分按照 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。

本部分由中华人民共和国工业和信息化部提出。

本部分由中华人民共和国工业和信息化部(通信)归口。

本部分起草单位：中国信息通信研究院、阿里云计算有限公司、华为技术有限公司、济源市信息中心、北京易华录信息技术股份有限公司、北京金山网络科技有限公司、中兴通讯股份有限公司、福建伊时代信息科技股份有限公司、东莞中国科学院云计算产业技术创新与育成中心、西安未来国际信息股份有限公司、山东中创软件商用中间件股份有限公司、首都信息发展股份有限公司。

本部分主要起草人：谢玮、沈锡镛、张彦超、徐浩、谢学广、吕铭、董文兴、陈桂华、邓金侠、任春林、林凯、赵伟、孙应娥、刘宇鹏。

引 言

电子政务发展正处于转变发展方式、深化应用和突出成效的关键转型期。政府职能转变和服务型政府建设对电子政务发展提出了更新更高要求。以云计算为代表的新兴信息技术、产业、应用不断涌现,深刻改变了电子政务发展技术环境及条件。构建基于云计算的电子政务公共平台可以充分发挥既有资源的作用和新兴信息技术潜能,加快电子政务发展创新,提高应用支撑服务能力,增强安全保障能力,减少重复建设、避免各自为政和信息孤岛。

基于云计算的电子政务公共平台上承载的信息资源是指与业务应用相关的信息数据,涉及国家安全、社会稳定和用户利益。为加强对电子政务公共平台信息资源的安全管理,使信息资源的管理工作系统化、规范化,特制定本部分。

本部分在基于云计算的电子政务公共平台安全体系框架下,充分考虑云计算技术应用带来的信息安全风险,根据公共平台信息资源受访的限制程度对安全保护场景实施分类,并针对不同类别对电子政务公共平台信息资源的访问、传输、存储及环境、备份和恢复、隔离、销毁、迁移等全生命周期的安全保障提出相应的要求,同时提出明确的安全管理技术要求。

基于云计算的电子政务公共平台安全规范

第 2 部分：信息资源安全

1 范围

GB/T 34080 的本部分规定了基于云计算的电子政务公共平台上承载的信息资源的访问、传输、存储及环境、备份和恢复、隔离、销毁、迁移的安全保障与管理要求。

本部分适用于基于云计算的电子政务公共平台的信息资源安全保障技术部署、安全运维管理和安全管理等方面。

注：除非特殊说明，以下各章中“电子政务公共平台”均指“基于云计算的电子政务公共平台”。

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 34078.1—2017 基于云计算的电子政务公共平台总体规范 第 1 部分：术语和定义

GB/T 34080.1—2017 基于云计算的电子政务公共平台安全规范 第 1 部分：总体要求

3 术语、定义和缩略语

3.1 术语和定义

GB/T 34078.1—2017 和 GB/T 34080.1—2017 界定的以及下列术语和定义适用于本文件。

3.1.1

电子政务公共平台服务提供机构 service provider of EGCP

负责提供和保证电子政务公共平台正常运行和服务的专业技术服务机构。

3.1.2

电子政务公共平台服务使用机构 serviceusing organization of EGCP

向电子政务公共平台申请服务及资源、开展政务应用的各政务部门。

3.1.3

电子政务公共平台信息资源所有者 owner of information resource of EGCP

电子政务公共平台上所承载信息资源的法律意义上的所有权机构(通常情况,即指将信息资源承载在电子政务公共平台上,并通过电子政务公共平台开展政务应用的各政务部门)。

3.2 缩略语

下列缩略语适用于本文件。

ACL:访问控制列表(Access Control List)

ARP:地址解析协议(Address Resolution Protocol)

DDoS:分布式拒绝服务攻击(Distributed Denial of Service)

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

- ID:身份标识(Identity)
- IP:互联网协议(Internet Protocol)
- IPsec:互联网协议安全(Internet Protocol Security)
- SSH:安全外壳协议(Secure Shell)
- SSL:安全套接层(Secure Sockets Layer)
- URL:统一资源定位符(Uniform Resource Locator)
- VLAN:虚拟局域网(Virtual Local Area Network)
- VPN:虚拟专用网络(Virtual Private Networks)
- SFTP:安全文件传送协议(Secure File Transfer Protocol)

4 电子政务公共平台信息资源范畴

电子政务公共平台中的信息资源是指平台承载的业务应用相关的信息数据,包括基础实体数据、用户及权限数据、业务应用数据、业务流转数据、业务输出数据、共享支撑数据、机构目录数据和对基础实体数据经过再处理后的数据等。

5 电子政务公共平台信息资源安全保护分类

电子政务公共平台自身的安全保障遵循国家信息系统等级保护要求,应根据电子政务公共平台建设及运行后的实际情况确定其安全级别,并实施相应的安全保护措施。电子政务公共平台上承载的信息资源以及其所属政务部门(电子政务公共平台服务使用机构)的业务系统,也应依据其系统的使命、目标和重要程度,确定安全等级,并由电子政务公共平台以安全服务形式提供满足其安全等级相应要求的安全保障能力。

同时,考虑到基于云计算的电子政务公共平台的特性,本部分将电子政务公共平台信息资源根据其受访的限制程度分为以下四类安全保护场景,见表 1 所述。

表 1 信息资源安全保护分类

分类定义	类别
信息资源经过信息资源所有者授权后可对所有社会公众用户开放	1
信息资源经过信息资源所有者授权后对指定社会公众用户开放	2
信息资源经过信息资源所有者授权后对指定电子政务公共平台服务使用机构开放	3
信息资源仅对信息资源所有者开放	4
注:“开放”的范围及权限由信息资源所有者决定。	

6 电子政务公共平台信息资源安全保护要求

6.1 第 1 类

6.1.1 信息资源访问

本项要求包括:

- a) 信息资源的安全访问策略需由授权主体配置,执行最小化授权原则,授予不同平台服务使用者

为完成各自任务所需的最小权限,并在它们之间形成相互制约的关系。

- b) 访问控制的覆盖范围应包括与信息资源访问相关的主体、客体及它们之间的操作。
- c) 应为电子政务公共平台服务使用者提供服务管理界面,支持云安全域或安全组划分,允许平台服务使用者灵活定义访问控制策略。
- d) 存储信息资源的环境应具备抵御分布式拒绝服务攻击和应用攻击的防御能力,防御架构应具备高弹性、可扩展能力,保证平台防御能力不随平台服务使用者增加而降低性能。
- e) 应具备异常流量检测、流量调度、流量清洗能力,为电子政务公共平台提供的云服务和平台服务使用者提供实时恶意流量清洗,清洗范围包括网络层、传输层、应用层的拒绝服务攻击、垃圾邮件等。
- f) 应严格限制由内部发起的对外连接,对内部采取必要的安全措施,进行内部行为监控。
- g) 应在电子政务公共平台边界处提供网络入侵检测措施,对来自电子政务公共平台外部的入侵事件进行检测和预警,并能够记录入侵事件的来源、目的、入侵时间、入侵类型等。
- h) 应对来自电子政务公共平台外部和平台内部的应用安全事件进行实时监测和预警,应用安全事件应包括网页篡改、网页挂马、敏感信息发布、应用可用性故障等,例如可采用流量重定向技术实现。

6.1.2 信息资源传输

本项要求包括:

- a) 应实现对电子政务公共平台内部主机和应用的访问进行控制,防火墙应支持对虚拟机实例的访问进行控制,例如可采用虚拟防火墙或流量重定向到物理防火墙技术实现。
- b) 应能够检测到信息资源在传输过程中完整性受到破坏,并在检测到完整性错误时采取必要的恢复措施。
- c) 应可限制网络最大网络流量数及网络连接数,限制恶意攻击流量,确保为高级别访问预留足够带宽。
- d) 应可以对传输目的地设置灵活的 ACL,从认证、时间、VLAN、IP 等多个角度进行限定。
- e) 应采用数字签名等技术,保证数据传输中不被篡改。

6.1.3 信息资源存储

本项要求包括:

- a) 应部署病毒防护系统对承载信息资源的虚拟机实例进行恶意代码与病毒查杀,为所有平台服务使用者提供病毒检测和查杀服务,病毒查杀时主机性能不能明显降低,例如可采用虚拟机实例查杀等技术。
- b) 应部署漏洞扫描系统对承载信息资源的环境进行漏洞检查,定期对网络、主机、应用实施漏洞扫描,扫描范围包括操作系统漏洞、数据库漏洞、中间件漏洞、应用系统漏洞等。
- c) 应确保不同平台服务使用者之间的存储数据安全隔离,保障信息资源的可靠性,例如可采用碎片化分布式离散存储技术或其他安全隔离技术保存平台服务使用者数据。
- d) 应提供有效的硬盘保护方法,保证即使硬盘被窃取,非法用户也无法从硬盘中获取有效的平台服务使用者数据。
- e) 应能够检测到信息资源在存储过程中完整性受到破坏,并在检测到完整性错误时采取必要的恢复措施。

6.1.4 信息资源备份和恢复

本项要求包括:

GB/T 34080.2—2017

- a) 应提供本地数据备份与恢复功能,完全数据备份至少每天一次,备份介质场外存放。
- b) 应提供异地数据备份功能,利用通信网络将关键数据定时批量传送至备用场地。
- c) 应提供虚拟机自动恢复能力。
- d) 应提供主流应用的容灾保护,并支持容灾分权分域管理,根据不同的角色管理不同的容灾策略和恢复计划。
- e) 在信息资源所有者有相关安全要求的情况下,必要时应建立异地灾难备份中心,提供异地实时备份功能。

6.1.5 信息资源隔离

本项要求包括:

- a) 应采用有效技术保证实现不同云服务器虚拟化实例的隔离。
- b) 应保证云服务对物理资源的调度和管理均在平台虚拟化层内完成,可采用虚拟化重定向技术隔离平台内承载信息资源的云服务对平台物理资源的直接访问。
- c) 同一物理资源主机上的不同虚拟化实例的计算资源应有效隔离,避免不同虚拟化实例对计算资源争抢。
- d) 应保证云服务的虚拟内存地址具备唯一性,可采用内存独占模式隔离平台内同一物理资源主机上的不同虚拟化实例的内存资源。
- e) 应保证相对隔离的不同平台服务使用者的云服务虚拟化实例的防护安全,如可采用虚拟防火墙或安全组等技术保障不同平台服务使用者的云服务虚拟化实例隔离安全。
- f) 应通过网络隔离技术和流量清洗技术实现网络资源的隔离和过量占用。
- g) 应对平台虚拟化层运维操作进行实时监控和审计,对系统管理员和审计管理员账号及权限分离。
- h) 在信息资源所有者有相关安全要求的情况下,必要时可采用专用集群或者物理隔离技术实现不同业务系统之间信息资源的隔离。

6.1.6 信息资源销毁

本项要求包括:

- a) 应提供有效的技术手段清除需要销毁的数据及其所有副本,销毁过程应该有记录。
- b) 应提供技术手段(如数据覆盖等)禁止被销毁数据的恢复。

6.1.7 信息资源迁移

本项要求包括:

- a) 应制定信息资源迁移实施方案,并进行迁移方案可行性评估与风险评估,制定信息资源迁移风险控制措施,做好信息资源备份以及恢复相关工作,保证数据迁移不影响业务应用的连续性。
- b) 应支持数据的迁入和迁出安全确认机制,数据迁入时,应采用安全扫描技术,确认资源是否被恶意感染,如木马植入、病毒等信息;数据导出时,应防止资源迁出时泄露,可采用安全传输技术,如 IPsec VPN, SFTP 或本地传输机制。
- c) 信息资源迁移应进行数据一致性校验,并保证业务系统正常运行。
- d) 应对非标准格式的信息资源数据,提供转换工具或者技术文档说明专有格式,保证启用或弃用该云服务时,数据能迁入和迁出。
- e) 数据迁移过程中应根据平台服务使用者需求提供数据加密迁移能力。

6.2 第2类

6.2.1 信息资源访问

本项要求除第1类要求外,还包括:

- a) 应采用基于用户组或角色的方法,保障客体访问资源时权限明确。
- b) 应采用用户名、口令方式,提供信息资源访问的身份鉴别,口令应包含数字、字母(大小写)、特殊符号,口令长度不低于8位,应定期更换口令。
- c) 应采用必要的措施使平台服务使用者的访问和修改等行为具有不可抵赖性。
- d) 应采用加密方式存储平台服务使用者的口令信息。
- e) 应严格设置登录策略,按安全策略要求具备防范账户遭到暴力破解攻击的能力(如,对空口令、连续的某个字符等弱口令的自动检测;限定平台服务使用者连续错误输入密码次数,超过设定阈值,对平台服务使用者进行锁定,并设定锁定时间,在锁定时间内被锁定的平台服务使用者需通过注册时的标志信息进行密码重新设定或者凭有效证件进行设定)。
- f) 当进行访问权限更改时(如密码重置、密码找回等),应设置相关策略,防止暴力破解攻击。
- g) 应采用加密或签名等安全技术,保障信息资源访问的应用编程接口安全,访问接口至少应包含访问ID、签名算法、加密强度等参数。
- h) 应采用网络、数据库、应用等审计技术对信息资源进行监测、记录。
- i) 应提供登录统计与分析功能,以发现潜在威胁。

6.2.2 信息资源传输

本项要求除第1类要求外,还包括:

应采用传输层加密技术保证平台服务使用者端到平台端的信息资源访问通信安全,如SSL、SSH等。

6.2.3 信息资源存储

本项要求除第1类要求外,还包括:

应信息资源所有者要求,可提供采用符合国家认定的密码算法对数据进行存储加密保护的服务,平台服务商不得掌握密钥。

6.2.4 信息资源备份和恢复

同第1类要求。

6.2.5 信息资源隔离

同第1类要求。

6.2.6 信息资源销毁

本项要求除第1类要求外,还包括:

应采用磁盘消磁技术实现平台内物理资源主机在弃置、维修前的数据彻底删除,对光盘进行物理粉碎,并无法恢复。

6.2.7 信息资源迁移

同第1类要求。

6.3 第3类

6.3.1 信息资源访问

本项要求除第1类要求外,还包括:

- a) 应采用基于用户组或角色的方法,保障平台服务使用者访问资源时权限明确。
- b) 应采用第三方可信认证证书或动态令牌技术提供信息资源访问的身份鉴别。
- c) 应采用必要的措施使平台服务使用者的访问和修改等行为具有不可抵赖性。
- d) 应严格设置登录策略,按安全策略要求具备防范账户暴力破解攻击措施的能力(如限定平台服务使用者连续错误输入密码次数,超过设定阈值,对平台服务使用者进行锁定,并设定锁定时间,在锁定时间内被锁定的平台服务使用者需通过注册时的标志信息进行密码重新设定或者凭有效证件进行设定)。
- e) 当进行访问权限更改时(如密码重置、密码找回等),应设置相关策略,防止暴力破解攻击。
- f) 应采用国家密码管理局鉴定的对称加密技术或签名技术,保障信息资源访问的应用编程接口安全,密钥强度不低于128位,访问接口至少应包含访问ID、签名算法、加密强度等参数。
- g) 应采用登录监控审计技术实时监控信息资源访问行为,阻断非授权操作;应采用网络访问控制监控系统自动化发现非授权的对外端口开启和通信协议启用。

6.3.2 信息资源传输

本项要求除第1类要求外,还包括:

- a) 应采用传输层加密技术保证平台服务使用者端到平台端的信息资源访问通信安全,如SSL、SSH等。
- b) 应采用虚拟局域网技术或专线互联技术保证平台服务使用者端到平台端的信息资源访问通信安全。

6.3.3 信息资源存储

本项要求除第2类要求外,还包括:

- a) 应采用碎片化分布式离散存储技术保存平台内信息资源数据。
- b) 应具备平台内数据完整性验证机制,可检测到虚拟化实例镜像文件、系统管理数据、平台服务使用者身份鉴别信息和平台服务使用者信息资源数据在平台内存储的完整性。
- c) 应对重要信息资源设置敏感标记,并对有敏感标记的资源操作进行严格控制。

6.3.4 信息资源备份和恢复

同第1类要求。

6.3.5 信息资源隔离

同第1类要求。

6.3.6 信息资源销毁

本项要求除第1类要求外,还包括:

- a) 应支持磁盘高级清零技术实现平台服务使用者的删除数据要求。
- b) 应采用磁盘消磁技术实现平台内物理资源主机在弃置、维修前的数据彻底删除,并无法复原。

6.3.7 信息资源迁移

同第 1 类要求。

6.4 第 4 类

6.4.1 信息资源访问

本项要求除第 3 类要求外,还包括:

- a) 应采用第三方可信认证证书、动态令牌技术或多因子身份认证技术提供信息资源访问的身份鉴别。
- b) 应采用国家密码管理局鉴定的对称加密技术或签名技术,保障信息资源访问的应用编程接口安全,密钥强度不低于 256 位,访问接口至少应包含访问 ID、签名算法、加密强度等参数。
- c) 应采用网络准入技术和登录监控审计技术来阻止非授权者的入网和访问,对授权平台服务使用者的操作进行记录。
- d) 应采用必要的措施使平台服务使用者的访问和修改等行为具有不可抵赖性。
- e) 应采用访问域限制技术,保障平台服务使用者只能在特定环境下对信息资源访问,如服务器 ID、域名等信息,限制信息资源的访问环境。

6.4.2 信息资源传输

本项要求除第 3 类要求外,还包括:

需采用国家密码管理局鉴定的专用的加密设备保障广域网传输的安全性。

6.4.3 信息资源存储

本项要求除第 3 类要求外,还包括:

- a) 应采用国家密码管理局鉴定的密码算法,采用多重密钥保护机制对数据进行存储加密保护。
- b) 应提供文件级细粒度安全存储,可单独设置文件的密级、加密算法、加密密钥等。

6.4.4 信息资源备份和恢复

同第 1 类要求。

6.4.5 信息资源隔离

同第 1 类要求。

6.4.6 信息资源销毁

本项要求除第 3 类要求外,还包括:

销毁过程全程视频记录,视频记录长期(至少 6 个月)保持。

6.4.7 信息资源迁移

同第 1 类要求。

7 电子政务公共平台信息资源安全管理技术要求

7.1 日常监测要求

本项要求包括:

- a) 应根据监测指令对电子政务公共平台的双向流量数据进行监测,对发现的违法信息进行记录,违法信息监测发现形成监测日志,并及时上报。根据 IP 地址、域名、URL 地址、违法关键词等条件设置监测规则。
- b) 应根据过滤指令对电子政务公共平台的双向流量数据进行监测,对发现的违法信息进行过滤处置,并进行记录,形成过滤日志,及时上报。根据 IP 地址、域名、URL 地址、关键词等条件设置过滤规则。
- c) 应支持对流量异常等状态进行监测,分析异常产生的原因。
- d) 应定期对监测和报警记录进行分析、评审,发现可疑行为,形成分析报告,并采取必要的应对措施。
- e) 对通过电子政务公共平台接入系统对公众发布的信息内容应具备实时安全监控能力,并进行日志留存。
- f) 对电子政务公共平台管理员进行审计,经过认证的管理员才能够登录配置设备,并全程记录管理行为。
- g) 应定期对运行日志和审计数据进行分析,以便及时发现异常行为。
- h) 对使用加密传输技术的信息资源,应具备有效的手段进行违法信息的发现与处置。
- i) 应具备对超大流量数据的监测与过滤能力。
- j) 应具备对信息资源和资源服务可用性的监测功能和备份正确性校验功能,并对备份系统定期进行恢复演练。

7.2 安全审计要求

本项要求包括:

- a) 应能对以下事件生成审计日志:
 - 1) 管理员和平台服务使用者鉴别;
 - 2) 管理员和平台服务使用者的操作行为;
 - 3) 管理员和平台服务使用者授权序列的记录,以供追溯;
 - 4) 网络访问控制,包括平台、虚拟机和数据库的远程连接、远程操作、远程数据传输进行记录及审计。
- b) 审计日志应包括事件类型、事件时间、事件主体、事件客体、平台服务使用者 IP、事件成功/失败、事件详细信息等字段。
- c) 应提供审计日志的可选择查询功能,支持按以下条件之一或组合进行查询:事件类型、事件时间、触发事件用户、事件主体查询。
- d) 应保护审计日志不被未授权的访问、修改和破坏。
- e) 所有审计日志能被理解。
- f) 审计日志应存储在掉电非遗失性存储介质中,当存储空间被耗尽时,应采取相应措施,保证审计日志不丢失。
- g) 应提供对审计日志的导出和清空功能。

7.3 定位溯源要求

本项要求包括:

- a) 应建立数据资源定位溯源技术能力,能准确定位存在信息安全问题的应用或服务的源头,并保存相关记录,及时上报相关管理部门。
- b) 应启用数据溯源机制,对非溯源数据进行警示。
- c) 应具备出现问题之后可以立即启用溯源的技术手段,确保溯源的及时有效。

7.4 日志留存要求

本项要求包括：

- a) 应针对电子政务公共平台的流量数据监测行为形成监测日志和过滤日志。
- b) 监测日志和过滤日志记录至少包括源/目的 IP,源/目的端口、违法信息、采集时间以及触发监测动作的监测指令标识,对 HTTP 协议还需要记录 URL,存在代理行为的需要记录代理类型、代理 IP。
- c) 应提供界面良好的日志查询功能,可依据时间、IP 地址、URL 等进行独立或条件组合查询。
- d) 日志留存的信息存储应当与其他业务系统进行有效隔离,日志留存信息以文件形式存储时,应采用安全、便捷的文件存储格式,如采用二进制文件格式进行存储。
- e) 应记录系统管理员的操作日志,日志记录至少应包括:操作用户、操作时间、操作用户 IP 地址、操作内容等日志信息,并定期对操作日志进行审计。
- f) 对平台服务使用者信息、日志信息等负有保密义务,不得出售、篡改、故意泄露或违法使用用户及日志信息。
- g) 平台服务使用者访问日志留存时间不少于 6 个月,对第 3 类、第 4 类信息资源的访问日志以及所有类别信息资源操作日志都应长期保存。

7.5 应急处置要求

本项要求包括：

- a) 应建立相应的应急处置技术能力,可对存在信息安全问题的应用或服务及时处理。
- b) 在紧急情况下,应能够停止全部或部分服务,并保存相关记录,及时上报相关管理部门。
- c) 应制定应急响应预案,并定期进行应急演练。

7.6 安全风险评估要求

本项要求包括：

- a) 应定期对电子政务公共平台信息资源的安全性进行风险评估和安全技术加固。
 - b) 应根据风险评估结果制定相应的风险处理计划。
-

中 华 人 民 共 和 国
国 家 标 准
基于云计算的电子政务公共平台安全规范
第 2 部分：信息资源安全
GB/T 34080.2—2017

*

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 1 字数 24 千字
2017 年 7 月第一版 2017 年 7 月第一次印刷

*

书号：155066 • 1-56355 定价 18.00 元



GB/T 34080.2—2017