

---

# 网络安全标准化工作概要

中国科学院大学

赵战生

**2017年9月22日**

---

# 提纲

---

- 标准的作用及其重要性
  - TC260的机构机制
  - 标准化工作的成绩
  - 新标准在路上
  - 适应新形势的顶层设计
-

---

# 标准的作用及其重要性

---

# 标准的作用及其重要性

---

- ❑ 信息安全标准体现了人们对信息安全的意识、认识和共识。
  - ❑ 大规模的生产、部署信息安全技术产品、服务和管理，需要具有共识的技术规范和管理措施。
  - ❑ 工欲善其事，必先利其器。
  - ❑ 没有规矩不能成方圆。
  - ❑ 标准发挥着基础性、规范性、引领性重要作用。
-

---

## □ **TC260**第一届主任曲维枝同志指出：

没有信息安全的信息化是危险的信息化；  
没有完善的信息安全标准，信息化建设中的产品、系统、工程就不能实现安全的互联、互通、互操作，就不能形成我国自主的信息安全产业，就不能构造出一个自主可控的信息安全保障体系，就难以保证国家信息安全和国家利益。

。

---

# 认识在提升

---

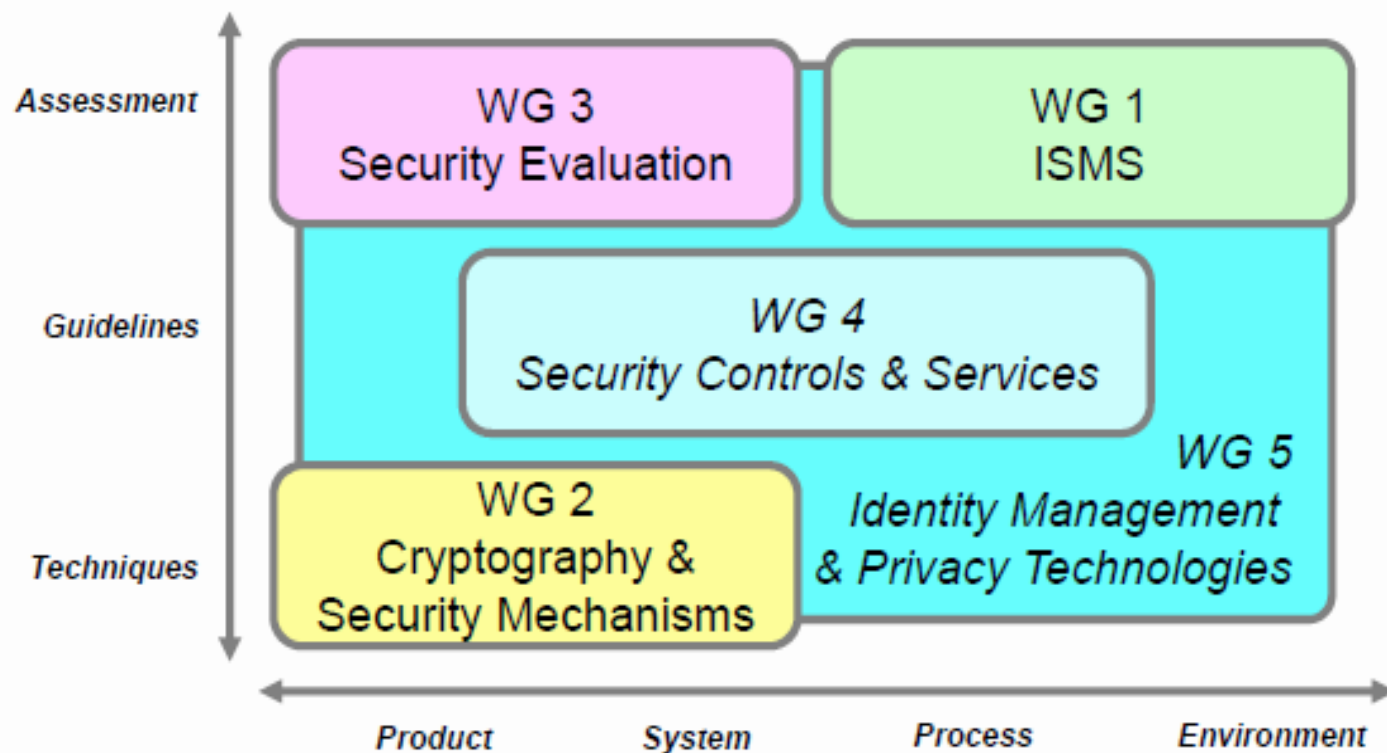
- 信息安全伴随信息化而生，在斗争博弈中成长，体现保障体系的对抗
  - 信息安全标准体系是信息安全保障体系的重要组成部分
    - 信息安全保障的基本制度性安排需要标准规范
    - 信息安全技术的产品、服务需要标准规范
    - 信息安全管理需要标准考察评估合规性
    - 新技术应用需要信息安全标准提升安全性
  - 标准化工作是维护国家主权，体现我国话语权，保安全，捍利益的重要阵地。
  - 中国需要从战略博弈的角度出发，推进网络安全技术标准制订和完善。
-

# ISO/IEC JTC1 SC27

## 信息安全标准化工作内容

---

- **WG1:** 信息安全管理体系
  - **WG2:** 密码学与安全机制
  - **WG3:** 安全评价准则
  - **WG4:** 安全控制与服务
  - **WG5:** 身份管理与隐私保护技术
-





---

# TC260的机构机制

---

# 完成了换届

---

## □ 组建了新一届标准化工作委员会班子

主任委员： 王秀军

副主任委员： 赵泽良    韩 俊    赵 林  
                  李守鹏    何良生    王京涛  
                  刘卫军

秘 书 长： 高 林

副秘书长： 杜 巍    刘贤刚

□ 委员：**81**人

□ 成员单位：**230**个

---

# 机构设置



# 完善了规章制度

---

- 1.** 全国信息安全标准化技术委员会章程
  - 2.** 全国信息安全标准化技术委员会工作组章程
  - 3.** 全国信息安全标准化技术委员会标准制修订工作程序
  - 4.** 信息安全国家标准项目管理办法
  - 5.** 信息安全国际标准化活动管理办法
-

## **WG1-信息安全标准体系与协调工作组**

---

- 任 务：研究信息安全标准体系；跟踪国际信息安全标准发展动态；研究、分析国内信息安全标准的应用需求；研究并提出新工作项目及工作建议。
  - 组 长：顾建国
  - 副组长：胡啸、高林
-

## WG2-涉密信息系统安全保密标准工作组

---

- 任 务：研究提出涉密信息系统安全保密标准体系；制定和修订涉密信息系统安全保密标准，以保证我国涉密信息系统的安全。
  - 组 长：马朝斌
  - 副组长：王文君、黄伟庆
-

# WG3-密码技术工作组

---

- 任 务：密码算法、密码模块，密钥管理标准的研究与制定。
  - 组 长：安晓龙
  - 副组长：刘平、詹榜华、谢永泉、李大为
-

# WG4-鉴别与授权工作组

---

- 任 务：国内外**PKI/PMI**标准的分析、研究和制定。
  - 组 长：荆继武
  - 副组长：詹榜华、李新友
-



# WG5-信息安全评估工作组

---

- 任 务：调研国内外测评标准现状与发展趋势；研究提出测评标准项目和制定计划。
  - 组 长：李京春
  - 副组长：顾健、李斌、李嵩
-

# WG6-通信安全标准工作组

---

- 任 务：调研通信安全标准现状与发展趋势，研究提出通信安全标准体系，制定和修订通信安全标准。
  - 组 长：于生多
  - 副组长：武冰梅、舒敏、郑志彬
-

# WG7-信息安全管理工作组

---

- 任 务：信息安全管理标准体系的研究,信息安全管理标准的制定工作。
  - 组 长：杨建军
  - 副组长：闵京华
-

# 大数据安全标准特别工作组

---

- 任 务：负责大数据和云计算相关的安全标准化研制工作。具体职责包括调研急需标准化需求，研究提出标准研制路线图，明确年度标准研制方向，及时组织开展关键标准研制工作。
  - 组 长：王建民
  - 副组长：陈兴蜀
-

# 秘书处基本信息

---

- 地址：中国，北京，安定门东大街一号 中国电子技术标准化研究院
  - 联系电话：**010-64102731、010-64102730**
  - 联系人：上官晓丽、许玉娜、黄馨蓓
  - 传真：**010-64102997**
  - 邮编：**100007**
-

# 启动了**2016**年度优秀网络安全国家标准奖评选活动

---

- 1. GB/T 22239-2008** 《信息安全技术 信息系统安全等级保护基本要求》 主要起草人：马力、任卫红、李明等。
  - 2. GB/T 29244-2012** 《信息安全技术 办公设备基本安全要求》 主要起草人：杨建军、陈星、高健等。
  - 3. GB/T 30278-2013** 《信息安全技术 政务计算机终端核心配置规范》 主要起草人：李新友、刘蓓、许涛等。
  - 4. GB/T 31168-2014** 《信息安全技术 云计算服务安全能力要求》 主要起草人：左晓栋、陈兴蜀、张建军等。
  - 5. GB/T 31167-2014** 《信息安全技术 云计算服务安全指南》 主要起草人：陈兴蜀、左晓栋、闵京华等。
-

# TC260工作机制

---

- 成员构成：产、学、研、用、管
  - 工作阶段：研究、预编、编制、宣贯
  - 工作流程：
    - 项目申请
    - 项目审批
    - 项目开展
      - 项目组阶段：编制报告，专家评审-征求意见稿。
      - 工作组阶段：征求意见，专家评审，成员投票-送审稿。
      - 秘书处阶段：委员会审查-报批稿。
      - 全标委阶段：审批，-颁布正式标准。
-

---

# 标准化工作的成绩

---



# 标准化工作的成绩

---

## □ 截止**2016**年底

- 发布标准**190**项
- 列入制修订计划**134**项

## □ **2016**年内

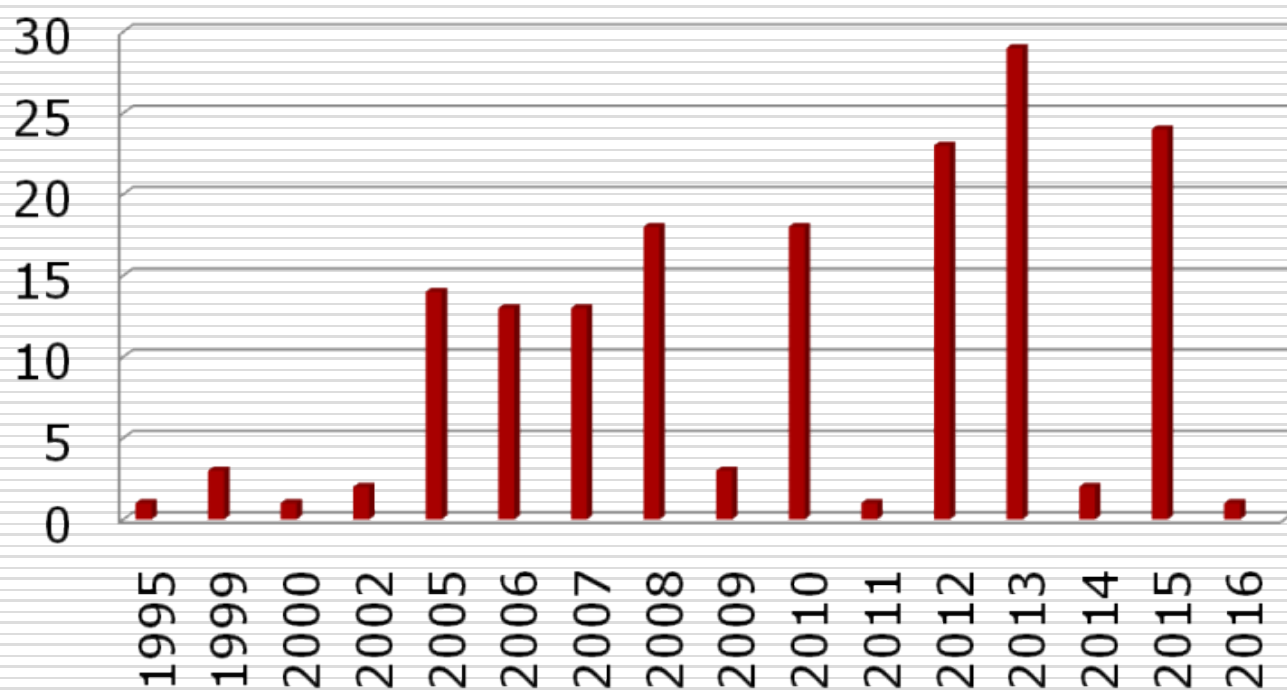
- 新发布标准**30**项
  - 完成报批稿**29**项
  - 新上制修订计划**21**项
-

# 我国信息安全保障工作的基本制度性安排

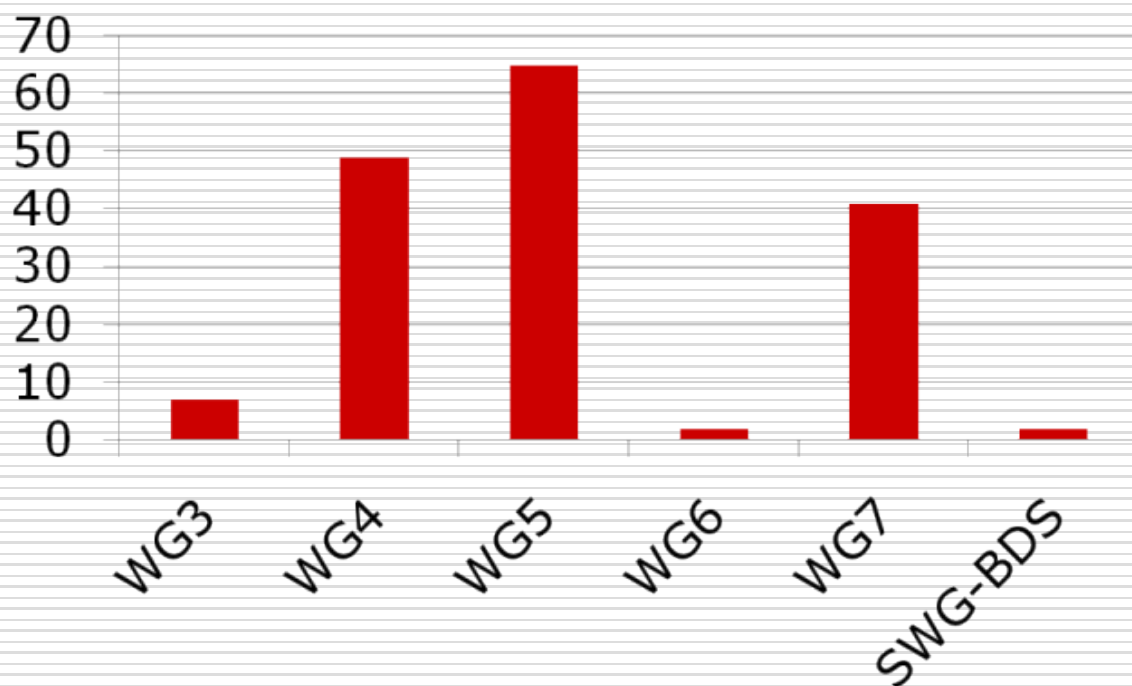
---

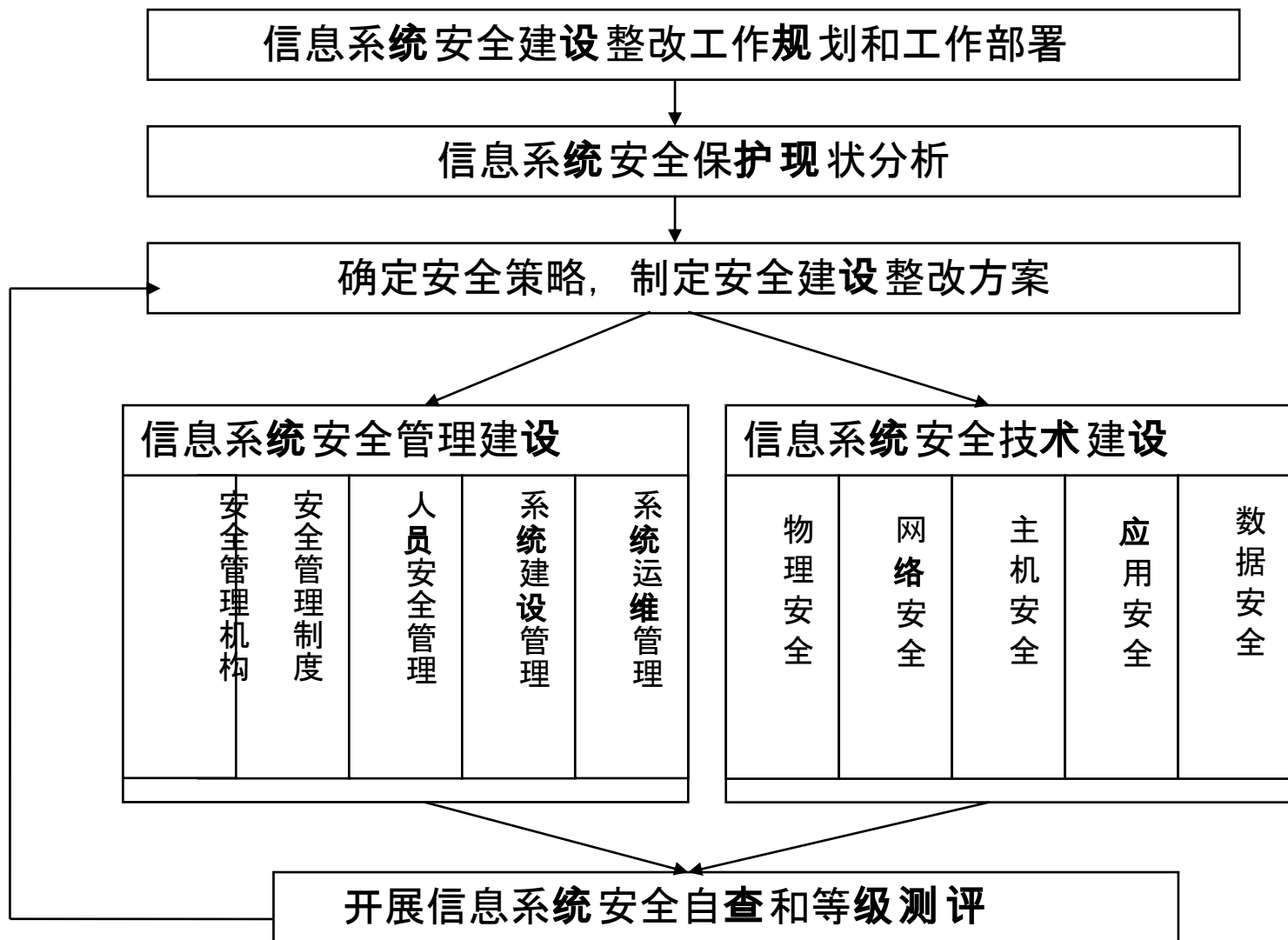
- 信息安全等级保护
  - 涉密信息系统的分级保护
  - 关键信息基础设施保护
  - 密码技术的研究、开发、应用、管理
  - 信息安全保障工作中的产品、服务认证认可
-

每年制定标准数



各工作组完成标准数量





# 等级保护依据的标准

---

## □ 指导定级：

- **GB 17859-1999** 《计算机信息系统 安全保护等级划分准则》
  - **GB/T 22240—2008** 《信息安全技术 信息系统安全等级保护定级指南》
  - **GB/T ××××—××××** 《信息安全技术 信息系统安全等级保护实施指南》
-

---

## □ 指导技术建设整改:

- **GB/T 20984—2007** 《信息安全技术 信息安全风险评估规范》
  - **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 XXXXX—XXXX** 《信息安全技术信息系统等级保护安全设计 技术要求》
  - **GB/T 20270—2006** 《信息安全技术 网络基础安全技术要求》
  - **GB/T 20271—2006** 《信息安全技术 信息系统安全通用技术要求》
  - **GB/T 21052—2007** 《信息安全技术 信息系统物理安全技术要求》
  - **GB/T 21053—2007** 《信息安全技术 公钥基础设施 **PKI** 系统安全等级保护技术要求》
  - **GB/T 18018—2007** 代替**GB/T 18018-1999** 《信息安全技术 路由器安全技术要求》
  - **GB/T 20979—2007** 《信息安全技术 虹膜识别系统技术要求》
  - **GB/T 21028—2007** 《信息安全技术 服务器安全技术要求》
-

- 
- **GB/T 20272—2006** 《信息安全技术 操作系统安全技术要求》
  - **GB/T 20273—2006** 《信息安全技术 数据库管理系统安全技术要求》
  - **GB/T 20275—2006** 《信息安全技术 入侵检测系统技术要求和测试评价方法》
  - **GB/T 20278—2006** 《信息安全技术 网络脆弱性扫描产品技术要求》
  - **GB/T 20279—2006** 《信息安全技术 网络和终端设备隔离部件安全技术要求》
  - **GB/T 20281—2006** 《信息安全技术 防火墙技术要求和测试评价方法》
  - **GA/T 708-2007** 《信息安全技术 信息系统安全等级保护体系框架》
  - **GA/T 709—2007** 《信息安全技术 信息系统安全等级保护基本模型》
  - **GA/T 710-2007** 《信息安全技术 信息系统安全等级保护基本配置》
  - **GA/T 711-2007** 《信息安全技术 应用软件系统安全等级保护通用技术指南》
  - **GA/T 712—2007** 《信息安全技术 应用软件系统安全等级保护通用测试指南》



---

## □ 指导管理建设整改

- **GB/T 20269—2006** 《信息安全技术 信息系统安全管理要求》
- **GA/T 713-2007** 《信息安全技术 信息系统安全管理测评》
- **GB/T 20282—2006** 《信息安全技术 信息系统安全工程管理要求》
- **GB/Z 20985—2007** 《信息技术 安全技术 信息安全事件管理指南》
- **GB/Z 20986—2007** 《信息安全技术 信息安全事件分类分级指南》
- **GB/T 20988—2007** 《信息安全技术 信息系统灾难恢复规范》

## □ 指导测评：

- **GB/T XXXX—XXXX** 《信息安全技术 信息系统安全等级保护测评要求》
- **GB/T ×××××—××××** 《信息安全技术 信息系统安全等级保护测评过程指南》



# 以密码为核心的网络信任体系建设的应用标准

|                          |                                    |
|--------------------------|------------------------------------|
| GB/T 17964-2008          | 《信息安全技术 分组密码算法的工作模式》               |
| GB/T 15843.1-2008        | 《信息技术 安全技术 实体鉴别 第1部分: 概述》          |
| GB/T 15843.2-2008        | 《信息技术 安全技术 实体鉴别 第2部分: 采用对称加密算法的机制》 |
| GB/T 15843.3-2008        | 《信息技术 安全技术 实体鉴别 第3部分: 采用数字签名技术的机制》 |
| GB/T 15843.4-2008        | 《信息技术 安全技术 实体鉴别 第4部分: 采用密码校验函数的机制》 |
| <b>GB/T 15843.5-2005</b> | 《信息技术 安全技术 实体鉴别 第5部分: 使用零知识技术的机制》  |
| GB/T 15852.1-2008        | 《信息技术 安全技术 消息鉴别码 第1部分: 采用分组密码的机制》  |
| GB/T 17903.1-2008        | 《信息技术 安全技术 抗抵赖 第1部分: 概述》           |
| GB/T 17903.2-2008        | 《信息技术 安全技术 抗抵赖 第2部分: 采用对称技术的机制》    |
| GB/T 17903.3-2008        | 《信息技术 安全技术 抗抵赖 第3部分: 采用非对称技术的机制》   |

---

|                   |                                   |
|-------------------|-----------------------------------|
| GB/T 19717-2005   | 《基于多用途互联网邮件扩展（MIME）的安全报文交换》       |
| GB/T 19771-2005   | 《信息技术 安全技术 公钥基础设施 PKI组件最小互操作规范》   |
| GB/T 19713-2005   | 《信息技术 安全技术 公钥基础设施 在线证书 状态协议》      |
| GB/T 19714-2005   | 《信息技术 安全技术 公钥基础设施 证书 管理协议》        |
| GB/T 20518-2006   | 《信息安全技术 公钥基础设施 数字证书 格式》           |
| GB/T 17902.2-2005 | 《信息技术 安全技术 带附录的数字签名 第2部分：基于身份的机制》 |
| GB/T 17902.3-2005 | 《信息技术 安全技术 带附录的数字签名 第3部分：基于证书的机制》 |
| GB/T 20520-2006   | 《信息安全技术 公钥基础设施 时间戳规范》             |
| GB/T 20519-2006   | 《信息安全技术 公钥基础设施 特定权限管理中心技术规范》      |

---

|                        |                                 |
|------------------------|---------------------------------|
| <b>GB/T 21054-2007</b> | 《信息安全技术 公钥基础设施 PKI系统安全等级保护评估准则》 |
| <b>GB/T 21053-2007</b> | 《信息安全技术 公钥基础设施 PKI系统安全等级保护技术要求》 |
| <b>GB/T 25057-2010</b> | 《信息安全技术 公钥基础设施 电子签名卡应用接口基本要求》   |
| <b>GB/T 25059-2010</b> | 《信息安全技术 公钥基础设施 简易在线证书 状态协议 》    |
| <b>GB/T 25060-2010</b> | 《信息安全技术 公钥基础设施 X.509数字证书应用接口规范》 |
| <b>GB/T 25061-2010</b> | 《信息安全技术 公钥基础设施 XML数字签名语法与处理规范》  |
| GB/T 25065-2010        | 《信息安全技术 公钥基础设施 签名生成应用程序的安全要求》   |
| GB/T 25056 - 2010      | 《信息系统安全技术 证书认证 系统密码及其相关安全技术规范》  |
| GB/T 25055 - 2010      | 《信息安全技术 公钥基础设施安全支撑平台技术框架》       |
| GB/T 25064 - 2010      | 《信息安全技术 公钥基础设施 电子签名格式规范》        |

# 密码的自主可控是国家安全的需要

---

□ **2012年3月21日**，国家密码管理局发布第 **23** 号公告，公开发布了我国的一系列密码算法和应用标准他们是

:

- **GM/T 0001-2012** 《祖冲之序列密码算法》
  - **GM/T 0002-2012** 《**SM4**分组密码算法》  
(原**SMS4**分组密码算法)
  - **GM/T 0003-2012** 《**SM2**椭圆曲线公钥密码算法》
  - **GM/T 0004-2012** 《**SM3**密码杂凑算法》
  - **GM/T 0005-2012** 《随机性检测规范》
  - **GM/T 0006-2012** 《密码应用标识规范》
-

# 国家密码管理局公告（第 24 号）

---

□ 发布国家密码管理局批准《**SM2**密码算法使用规范》等**14**项密码行业标准(**2012年11月22日**)

- **GM/T 0008-2012** 《安全芯片密码检测准则》
  - **GM/T 0009-2012** 《**SM2**密码算法使用规范》
  - **GM/T 0010-2012** 《**SM2**密码算法加密签名消息语法规范》
  - **GM/T 0011-2012** 《可信计算 可信密码支撑平台功能与接口规范》
  - **GM/T 0012-2012** 《可信计算 可信密码模块接口规范》
  - **GM/T 0013-2012** 《可信计算 可信密码模块符合性检测规范》
  - **GM/T 0014-2012** 《数字证书认证系统密码协议规范》
  - **GM/T 0015-2012** 《基于**SM2**密码算法的数字证书格式规范》
-

- 
- **GM/T 0016-2012** 《智能密码钥匙密码应用接口规范》
  - **GM/T 0017-2012** 《智能密码钥匙密码应用接口数据格式规范》
  - **GM/T 0018-2012** 《密码设备应用接口规范》
  - **GM/T 0019-2012** 《通用密码服务接口规范》
  - **GM/T 0020-2012** 《证书应用综合服务接口规范》
  - **GM/T 0021-2012** 《动态口令密码应用技术规范》
-

# 国家密码管理局公告（第 28 号）

---

□ 发布《**IPSec VPN**技术规范》等**17**项密码行业标准

- **GM/T 0022-2014** 《**IPSec VPN**技术规范》
  - **GM/T 0023-2014** 《**IPSec VPN** 网关产品规范》
  - **GM/T 0024-2014** 《**SSL VPN**技术规范》
  - **GM/T 0025-2014** 《**SSL VPN** 网关产品规范》
  - **GM/T 0026-2014** 《安全认证网关产品规范》
  - **GM/T 0027-2014** 《智能密码钥匙技术规范》
  - **GM/T 0028-2014** 《密码模块安全技术要求》
  - **GM/T 0029-2014** 《签名验签服务器技术规范》
  - **GM/T 0030-2014** 《服务器密码机技术规范》
  - **GM/T 0031-2014** 《安全电子签章密码技术规范》
  -
-



- 
- **GM/T 0032-2014** 《基于角色的授权管理与访问控制技术规范》
  - **GM/T 0033-2014** 《时间戳接口规范》
  - **GM/T 0034-2014** 《基于**SM2**密码算法的证书认证系统密码及其相关安全技术规范》
  - **GM/T 0035-2014** 《射频识别系统密码应用技术要求》
  - **GM/T 0036-2014** 《采用非接触卡的门禁系统密码应用技术指南》
  - **GM/T 0037-2014** 《证书认证系统检测规范》
  - **GM/T 0038-2014** 《证书认证密钥管理系统检测规范》
-

# 国家密码管理局公告（第 29 号）

---

□ 发布《密码模块安全检测要求》等**5**项密码行业标准**(2015年4月1日)**

- **GM/T 0039-2015** 密码模块安全检测要求
  - **GM/T 0040-2015** 射频识别标签模块密码检测  
准则
  - **GM/T 0041-2015** 智能**IC**卡密码检测规范
  - **GM/T 0042-2015** 三元对等密码安全协议测试  
规范
  - **GM/T 0043-2015** 数字证书互操作检测规范
-

# 国家密码管理局公告（第 30 号）

---

□ 发布《**SM9**标识密码算法》等**2**项密码行业标准(**2016**年**3**月**28**日)

■ **GM/T 0044-2016 SM9**标识密码算法

■ **GM/T 0045-2016** 金融数据密码机技术规范

---

# 国家密码管理局公告（第 31 号）

---

□ 发布《金融数据密码机检测规范》等**8**项密码行业标准**(2016年12月23日)**

- **GM/T 0046-2016** 金融数据密码机检测规范
  - **GM/T 0047-2016** 安全电子签章密码检测规范
  - **GM/T 0048-2016** 智能密码钥匙密码检测规范
  - **GM/T 0049-2016** 密码键盘密码检测规范
  - **GM/T 0050-2016** 密码设备管理 设备管理技术规范
  - **GM/T 0051-2016** 密码设备管理 对称密钥管理技术规范
  - **GM/T 0052-2016** 密码设备管理 **VPN**设备监察管理规范
  - **GM/T 0053-2016** 密码设备管理 远程监控与合规性检验接口数据规范
-

# 保密标准

---

□ 我国的保密标准均由国家保密局（**WG2**）负责制定。至今已经完成**30**项相关标准。他们是：

- 1. BMB1-1994** 《电话机电磁泄漏发射限值和测试方法》
  - 2. BMB2-1998** 《使用现场的信息设备电磁泄漏发射检查测试方法和安全判据》
  - 3. BMB3-1999** 《处理涉密信息的电磁屏蔽室的技术要求和测试方法》
  - 4. BMB4-2000** 《电磁干扰器技术要求和测试方法》
-

- 
- 5. BMB5-2000** 《涉密信息设备使用现场的电磁泄漏发射防护要求》
  - 6. BMB6-2001** 《密码设备电磁泄漏发射限值》
  - 7. BMB7-2001** 《密码设备电磁泄漏发射测试方法（总则）》
  - 8. BMB7.1-2001** 《电话密码机电磁泄漏发射测试方法》
  - 9. BMB8-2004** 《国家保密局电磁泄漏发射防护产品检测实验室认可要求》
  - 10. BMB10-2004** 《涉及国家秘密的计算机网络安全隔离设备的技术要求和测试方法》
-

- 
- 11. BMB11-2004** 《涉及国家秘密的计算机信息系统防火墙安全技术要求》
  - 12. BMB12-2004** 《涉及国家秘密的计算机信息系统漏洞扫描产品技术要求》
  - 13. BMB13-2004** 《涉及国家秘密的计算机信息系统入侵检测产品技术要求》
  - 14. BMB14-2004** 《涉及国家秘密的信息系统安全保密测评实验室要求》
  - 15. BMB15-2004** 《涉及国家秘密的信息系统安全审计产品技术要求》
-

---

**16. BMB16-2004** 《涉及国家秘密的信息系统安全隔离与信息交换产品技术要求》

**17. BMB17-2006** 《涉及国家秘密的信息系统分级保护技术要求》（部分代替**BMZ1—2000**）

☐ **18. BMB18-2006** 《涉及国家秘密的信息系统工程监理规范》

☐ **19. BMB19-2006** 《电磁泄漏发射屏蔽机柜技术要求 and 测试方法》

☐ **20. GGBB1-1999** 《信息设备电磁泄漏发射限值》

☐ **21. GGBB2-1999** 《信息设备电磁泄漏发射测试方法》

---



---

**22. BMZ1-2000** 《涉及国家秘密的计算机信息系统保密技术要求》（已被**BMB17—2006**和**BMB20—2007**代替）

**23. BMZ2-2001** 《涉及国家秘密的计算机信息系统安全保密方案设计指南》（已被**BMB23—2008**代替）

**24. BMZ3-2001** 《涉及国家秘密的计算机信息系统安全保密测评指南》（已被**BMB22—2007**代替）

**25. BMB9.1-2007** 《保密会议移动通信干扰器技术要求和测试方法》

**26. BMB9.2-2007** 《保密会议移动通信干扰器安装使用指南》

---

---

**27. BMB20-2007** 《涉及国家秘密的信息系统分级保护管理规范》（部分代替**BMZ1—2000**）

**28.BMB21-2007** 《涉及国家秘密的载体销毁与信息消除安全保密要求》

**29.BMB22-2007** 《涉及国家秘密的信息系统分级保护测评指南》（代替**BMZ3—2001**）

**30. BMB23-2008** 《涉及国家秘密的信息系统分级保护方案设计指南》（代替**BMZ2—2001**）

---

---

# WG7至2015年制定的标准

---

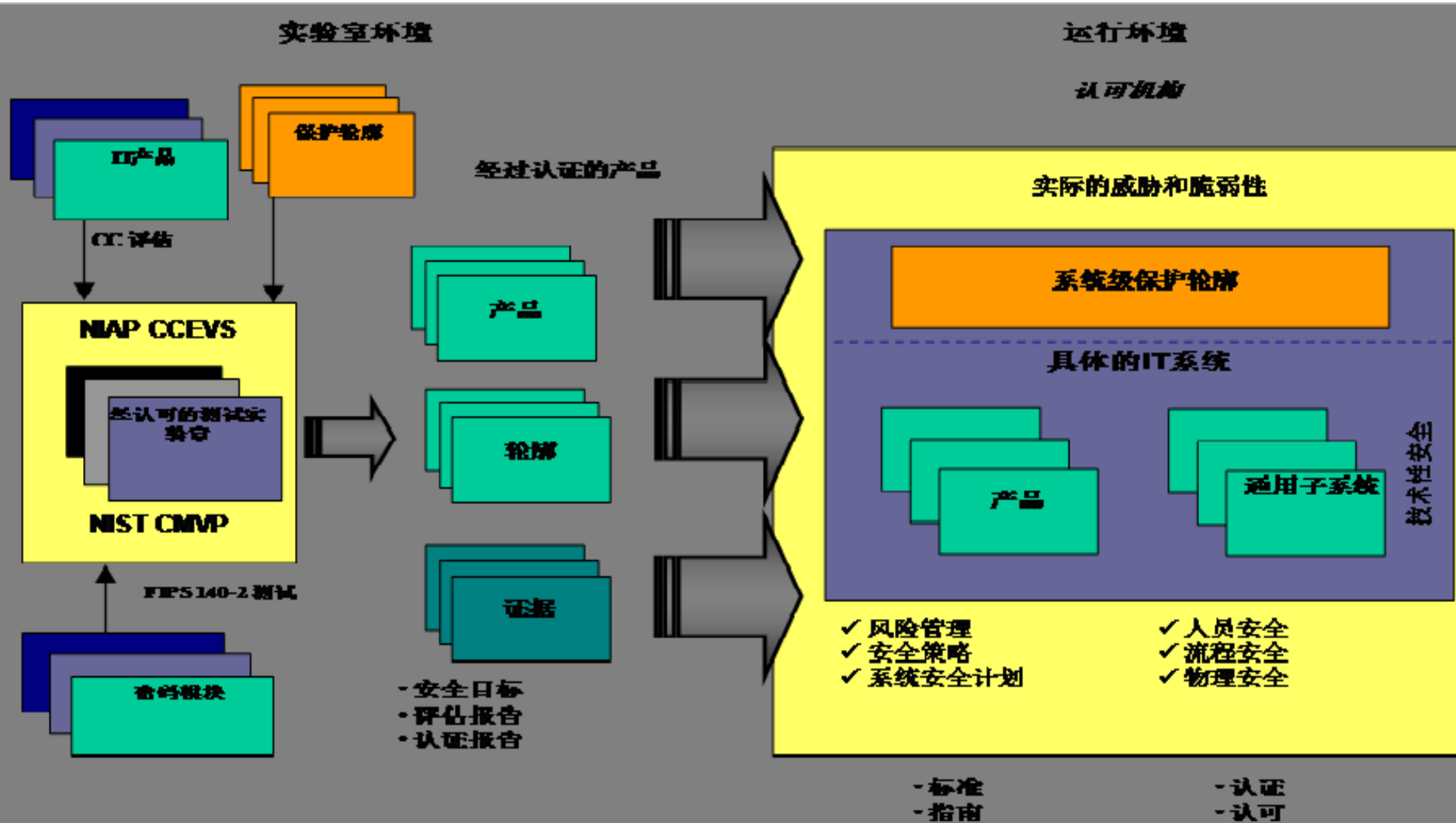
# 信息安全保障体系及评估方法

---

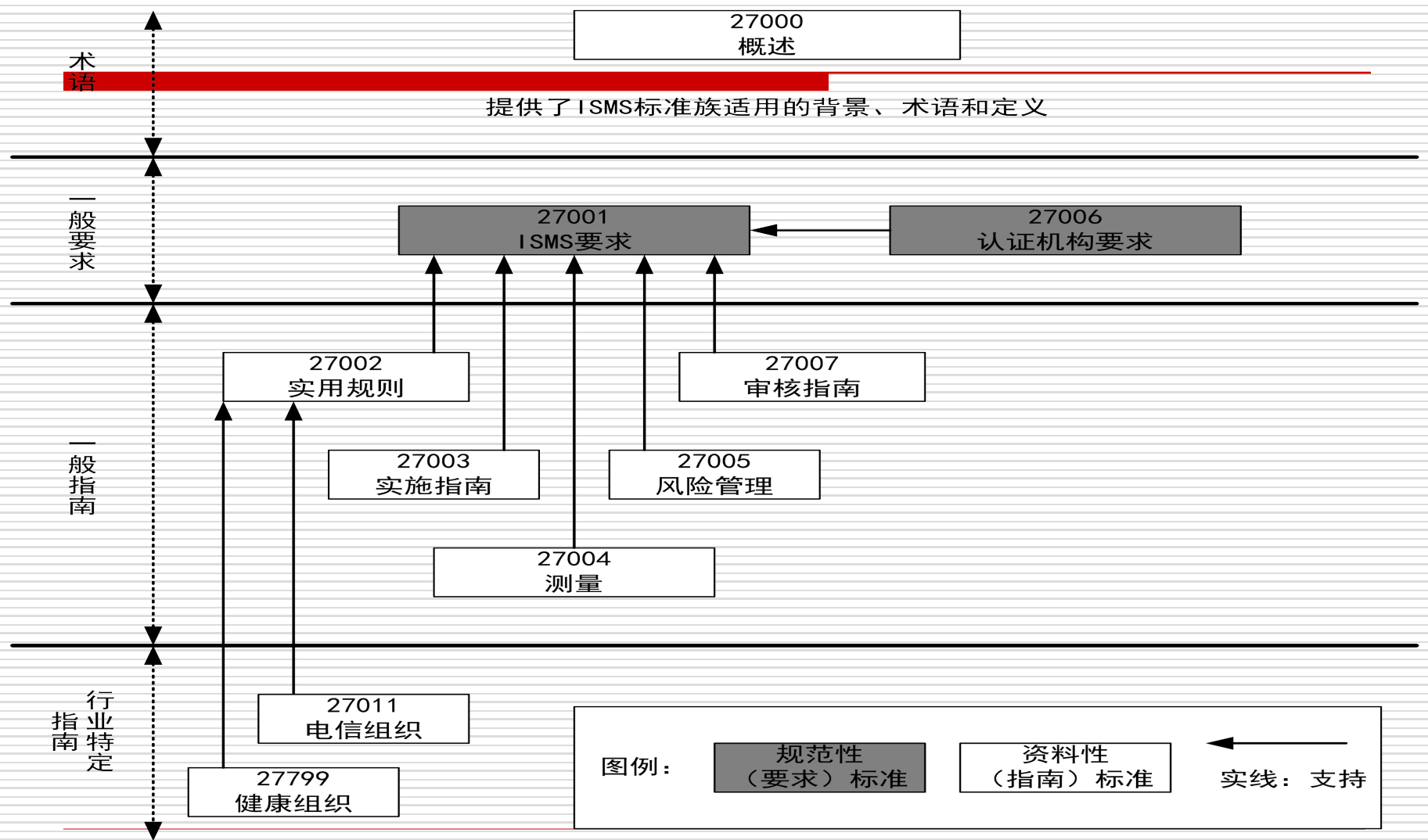
|                                   |                                                      |             |            |
|-----------------------------------|------------------------------------------------------|-------------|------------|
| <b>GB/T<br/>31495.2-<br/>2015</b> | <u>《信息安全技术 信息安全保障<br/>指标体系及评价方法 第2部分：<br/>指标体系》</u>  | <b>2015</b> | <b>WG7</b> |
| <b>GB/T<br/>31495.3-<br/>2015</b> | <u>《信息安全技术 信息安全保障<br/>指标体系及评价方法 第3部分：<br/>实施指南》</u>  | <b>2015</b> | <b>WG7</b> |
| <b>GB/T<br/>31495.1-<br/>2015</b> | <u>《信息安全技术 信息安全保障<br/>指标体系及评价方法 第1部分：<br/>概念和模型》</u> | <b>2015</b> | <b>WG7</b> |

---

# 技管并重风险管理体现了ISMS的要义



# 国际标准化组织信息安全管理标准 (ISMS) 家族 (27000系列)



# ISO/IEC 27000大家族为技管并重提供了规范性标准



# 信息系统安全管理体系（ISMS）

|                   |                                                    |      |     |
|-------------------|----------------------------------------------------|------|-----|
| GB/T 31497-2015   | <a href="#">《信息技术 安全技术 信息安全管理 测量》</a>              | 2015 | WG7 |
| GB/T 31722-2015   | <a href="#">《信息技术 安全技术 信息安全风险管理》</a>               | 2015 | WG7 |
| GB/T 31496-2015   | <a href="#">《信息技术 安全技术 信息安全管理体系实施指南》</a>           | 2015 | WG7 |
| GB/T 31509-2015   | <a href="#">《信息安全技术 信息安全风险评估实施指南》</a>              | 2015 | WG7 |
| GB/T 28450-2012   | <a href="#">《信息安全技术 信息安全管理体系审核指南》</a>              | 2012 | WG7 |
| GB/T 28453-2012   | <a href="#">《信息安全技术 信息系统安全管理评估要求》</a>              | 2012 | WG7 |
| GB/T 29246-2012   | <a href="#">《信息技术 安全技术 信息安全管理体系 概述和词汇》</a>         | 2012 | WG7 |
| GB/T 25067-2010   | <a href="#">《信息技术 安全技术 信息安全管理体系审核认证机构的要求》</a>      | 2010 | WG7 |
| GB/Z 24364-2009   | <a href="#">《信息安全技术 信息安全风险管理指南》</a>                | 2009 | WG7 |
| GB/T 22080-2008   | <a href="#">《信息技术 安全技术 信息安全管理体系 要求》</a>            | 2008 | WG7 |
| GB/T 22081-2008   | <a href="#">《信息技术 安全技术 信息安全管理实用规则》</a>             | 2008 | WG7 |
| GB/T 20984-2007   | <a href="#">《信息安全技术 信息安全风险评估规范》</a>                | 2007 | WG7 |
| GB/T 19715.1-2005 | <a href="#">《信息技术 信息技术安全管理指南 第1部分：信息技术安全概念和模型》</a> | 2005 | WG7 |
| GB/T 19715.2-2005 | <a href="#">《信息技术 信息技术安全管理指南 第2部分：管理和规划信息技术安全》</a> | 2005 | WG7 |



# 事件处理与灾难恢复

---

|                 |                                          |      |     |
|-----------------|------------------------------------------|------|-----|
| GB/Z 20986-2007 | <a href="#">《信息安全技术 信息安全事件分类分级指南》</a>    | 2007 | WG7 |
| GB/T 24363-2009 | <a href="#">《信息安全技术 信息安全应急响应计划规范》</a>    | 2009 | WG7 |
| GB/T 30285-2013 | <a href="#">《信息安全技术 灾难恢复中心建设与运维管理规范》</a> | 2013 | WG7 |
| GB/T 31500-2015 | <a href="#">《信息安全技术 存储介质数据恢复服务要求》</a>    | 2015 | WG7 |
| GB/Z 20985-2007 | <a href="#">《信息技术 安全技术 信息安全事件管理指南》</a>   | 2007 | WG7 |
| GB/T 20988-2007 | <a href="#">《信息安全技术 信息系统灾难恢复规范》</a>      | 2007 | WG7 |

# 配合等保信息管理系统管理要求

---

|                        |                                                                      |             |            |
|------------------------|----------------------------------------------------------------------|-------------|------------|
| <b>GB/T 20282-2006</b> | <u><a href="#">《信息安全技术 信息系统安全工程管</a></u> <u><a href="#">理要求》</a></u> | <b>2006</b> | <b>WG7</b> |
| <b>GB/T 20269-2006</b> | <u><a href="#">《信息安全技术 信息系统安全管理要求》</a></u>                           | <b>2006</b> | <b>WG7</b> |
| <b>GB/T 28453-2012</b> | <u><a href="#">《信息安全技术 信息系统安全管理评</a></u> <u><a href="#">估要求》</a></u> | <b>2012</b> | <b>WG7</b> |

---

# IT网络安全

---

|                   |                                                                 |      |     |
|-------------------|-----------------------------------------------------------------|------|-----|
| GB/T 25068.1-2012 | <a href="#"><u>《信息技术 安全技术 IT网络安全 第1部分：网络安全管理》</u></a>           | 2012 | WG7 |
| GB/T 25068.2-2012 | <a href="#"><u>《信息技术 安全技术 IT网络安全 第2部分：网络安全体系结构》</u></a>         | 2012 | WG7 |
| GB/T 25068.3-2010 | <a href="#"><u>《信息技术 安全技术 IT网络安全 第3部分：使用安全网关的网间通信安全保护》</u></a>  | 2010 | WG7 |
| GB/T 25068.4-2010 | <a href="#"><u>《信息技术 安全技术 IT网络安全 第4部分：远程接入的安全保护》</u></a>        | 2010 | WG7 |
| GB/T 25068.5-2010 | <a href="#"><u>《信息技术 安全技术 IT网络安全 第5部分：使用虚拟专用网的跨网通信安全保护》</u></a> | 2010 | WG7 |
| GB/T 28454-2012   | <a href="#"><u>《信息技术 安全技术 入侵检测 系统的选择、部署和操作》</u></a>             | 2012 | WG7 |

---

# 信息安全服务类

---

|                    |                                              |      |     |
|--------------------|----------------------------------------------|------|-----|
| GB/T<br>30271-2013 | <a href="#">《信息安全技术 信息安全服务能力评估准则》</a>        | 2013 | WG7 |
| GB/T<br>30283-2013 | <a href="#">《信息安全技术 信息安全服务 分类》</a>           | 2013 | WG7 |
| GB/Z<br>28828-2012 | <a href="#">《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》</a> | 2012 | WG7 |
| GB/T<br>28447-2012 | <a href="#">《信息安全技术 电子认证服务机构运营管理规范》</a>      | 2012 | WG7 |

---

# 可信计算类

---

|                        |                                                   |             |            |
|------------------------|---------------------------------------------------|-------------|------------|
| <b>GB/T 29827-2013</b> | <a href="#"><u>《信息安全技术 可信计算规范 可信平台主板功能接口》</u></a> | <b>2013</b> | <b>WG7</b> |
| <b>GB/T 29828-2013</b> | <a href="#"><u>《信息安全技术 可信计算规范 可信连接架构》</u></a>     | <b>2013</b> | <b>WG7</b> |
| <b>GB/T 29829-2013</b> | <a href="#"><u>《信息安全技术 可信计算密码支撑平台功能与接口规范》</u></a> | <b>2013</b> | <b>WG7</b> |

---

# 电子政务安全管理类

---

|                 |                                   |      |     |
|-----------------|-----------------------------------|------|-----|
| GB/T 29245-2012 | <u>《信息安全技术 政府部门信息安全管理基本要求》</u>    | 2012 | WG7 |
| GB/Z 24294-2009 | <u>《信息安全技术 基于互联网电子政务信息安全实施指南》</u> | 2009 | WG7 |

---

# 2017年新颁布的标准

---

- 1. GB/Z 24294.2-2017** 《信息安全技术 基于互联网电子政务信息安全实施指南 第2部分：接入控制与安全交换》（部分代替：**GB/Z 24294-2009**）
- 2. GB/Z 24294.3-2017** 《信息安全技术 基于互联网电子政务信息安全实施指南 第3部分：身份认证与授权管理》（部分代替：**GB/Z 24294-2009**）
- 3. GB/Z 24294.4-2017** 《信息安全技术 基于互联网电子政务信息安全实施指南 第4部分：终端安全防护》（部分代替：**GB/Z 24294-2009**）
- 4. GB/T 32918.5-2017** 《信息安全技术 **SM2**椭圆曲线公钥密码算法 第5部分：参数定义》
- 5. GB/T 33560-2017** 《信息安全技术 密码应用标识规范》
- 6. GB/T 33561-2017** 《信息安全技术 安全漏洞分类》
- 7. GB/T 33562-2017** 《信息安全技术 安全域名系统实施指南》
- 8. GB/T 33563-2017** 《信息安全技术 无线局域网客户端安全技术要求（评估保障级**2**级增强）》
- 9. GB/T 33565-2017** 《信息安全技术 无线局域网接入系统安全技术要求（评估保障级**2**级增强）》
- 10. GB/T 34095-2017** 《信息安全技术 用于电子支付的基于近距离无线通信的移动终端安全技术要求》

---

# 新标准在路上

---



---

## □ 工业控制系统

1. 《信息安全技术 工业控制系统产品信息安全通用评估准则》
  2. 《信息安全技术 工业控制系统漏洞检测技术要求及测试评价方法》
  3. 《信息安全技术 工业控制系统信息安全检查指南》
  4. 《信息安全技术 工业控制系统专用防火墙技术要求》
  5. 《信息安全技术 工业控制系统网络审计产品安全技术要求》
  6. 《信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求》
  7. 《信息安全技术 工业控制系统风险评估实施指南》
  8. 《信息安全技术 工业控制系统安全管理基本要求》
  9. 《信息安全技术 工业控制系统信息安全分级规范》
  10. 《信息安全技术 工业控制系统安全控制应用指南》
-

---

## □ 关键信息基础设施安全

1. 《信息安全技术 关键信息基础设施安全保障评价指标体系》
  2. 《信息安全技术 关键信息基础设施安全检查评估指南》
-

---

## □ 云计算安全

1. 《信息安全技术 桌面云安全技术要求》
  2. 《信息安全技术 云计算服务运行监管框架》
  3. 《信息安全技术 云计算安全参考架构》
  4. 《信息安全技术 云计算服务安全能力评估方法》
  5. 《信息安全技术 网站安全云防护平台技术要求》
-

---

## □ 物联网

1. 《信息安全技术 射频识别系统密码应用技术要求 第**1**部分：密码安全保护框架及安全级别》
  2. 《信息安全技术 射频识别系统密码应用技术要求 第**2**部分：电子标签与读写器及其通信密码应用技术要求》
  3. 《信息安全技术 物联网感知层接入信息网络的安全技术要求》
  4. 《信息安全技术 物联网数据传输安全技术要求》
  5. 《信息安全技术 物联网安全参考模型及通用要求》
  6. 《信息安全技术 物联网感知层网关安全技术要求》 《信息安全技术 物联网感知层网关安全技术要求》
  7. 《信息安全技术 物联网感知终端应用安全技术要求》
  8. 《信息安全技术 射频识别（**RFID**）系统通用安全技术要求》
-

---

## □ 移动通信

1. 《信息安全技术 移动签名通用技术规范》
  2. 《信息安全技术 移动终端安全管理平台技术要求》
  3. 《信息安全技术 移动互联网第三方应用服务器安全技术要求》
  4. 《信息安全技术 移动终端安全保护技术要求》
  5. 《信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法》
  6. 《信息安全技术 移动智能终端操作系统安全测试评价方法》
  7. 《信息安全技术 移动智能终端个人信息保护技术要求》
  8. 《信息安全技术 移动智能终端数据存储服务安全技术要求和测试评价方法》
  9. 《信息安全技术 低速无线个域网空口安全测试规范》
  10. 《信息安全技术 电子政务移动办公安全技术规范》
-

---

## □ 大数据

1. 《信息安全技术 大数据安全管理指南》
  2. 《信息安全技术 大数据服务安全能力要求》
  3. 《信息安全技术 数据出境安全评估指南》
  4. 《信息安全技术 智能音视频采集设备应用安全要求》
  5. 《信息安全技术 网络存储安全技术要求》
  6. 《信息安全技术 数据安全能力成熟度模型》
  7. 《信息安全技术 数据交易服务安全要求》
-

---

## □ 智慧城市

1. 《信息安全技术 智慧城市安全体系框架》
  2. 《信息安全技术 智慧城市建设信息安全保障指南》
-

# 网络安全等级保护

---

## □ 基本要求

1. 《信息安全技术 网络安全等级保护基本要求 第**1**部分：安全通用要求》
  2. 《信息安全技术 网络安全等级保护基本要求 第**2**部分：云计算安全扩展要求》
  3. 信息安全技术 网络安全等级保护基本要求 第**3**部分：移动互联安全扩展要求》
  4. 《信息安全技术 网络安全等级保护基本要求 第**4**部分：物联网安全扩展要求》
  5. 《信息安全技术 网络安全等级保护基本要求 第**5**部分：工业控制系统安全扩展要求》
  6. 信息安全技术 网络安全等级保护基本要求 第**6**部分 大数据安全扩展要求》
-



---

## □ 设计技术要求

1. 《信息安全技术 网络安全等级保护设计技术要求 第**1**部分：安全通用要求》
  2. 《信息安全技术 网络安全等级保护设计技术要求 第**2**部分：云计算安全扩展要求》
  3. 信息安全技术 网络安全等级保护设计技术要求 第**3**部分：移动互联安全扩展要求》
  4. 《信息安全技术 网络安全等级保护设计技术要求 第**4**部分：物联网安全扩展要求》
  5. 《信息安全技术 网络安全等级保护设计技术要求 第**5**部分：工业控制系统安全扩展要求》
  6. 信息安全技术 网络安全等级保护设计技术要求 第**6**部分 大数据安全扩展要求》
-

---

## □ 测评要求

1. 《信息安全技术 网络安全等级保护测评要求 第**1**部分：安全通用要求》
  2. 《信息安全技术 网络安全等级保护测评要求 第**2**部分：云计算安全扩展要求》
  3. 《信息安全技术 网络安全等级保护测评要求 第**3**部分：移动互联安全扩展要求》
  4. 《信息安全技术网络安全等级保护测评要求 第**4**部分：物联网安全扩展要求》
  5. 《信息安全技术网络安全等级保护测评要求 第**5**部分：工业控制系统安全扩展要求》
  6. 《信息安全技术网络安全等级保护测评要求 第**6**部分：大数据安全扩展要求》
-

---

## □ 其他

1. 《信息安全技术 网络安全等级保护测试评估技术指南》
  2. 《信息安全技术 网络安全等级保护测评过程指南》
  3. 《信息安全技术 网络安全等级测评机构能力要求和评估规范》
  4. 《信息安全技术 网络安全等级保护安全管理中心技术要求》
-

---

# 适应新形势的顶层设计

---

# 适应新形势的顶层设计

---

- 三部门文件《关于加强国家网络安全标准化工作的若干意见》解析
    - 国际和国外在信息安全保障方面加速出台了体系化的适应新技术新应用的大量安全标准。
    - 我们不能满足已有成绩，必须为适应新形势，配合我国信息安全战略和法规的要求进行进一步的标准化工作的顶层设计。
    - 文件以聚集正能量，弘扬主旋律的方式为适应新形势提出了我国信息安全标准化工作的方向、任务和措施。
-

---

## □ 涉及七个方面

- 1.** 工作机制
  - 2.** 标准体系建设
  - 3.** 提升标准质量和基础能力
  - 4.** 强化标准宣传实施
  - 5.** 加强国际标准化工作
  - 6.** 抓好标准化人才队伍建设
  - 7.** 做好资金保障
-

---

## □ 提出十九项措施

### 一、工作机制

- (1) 建立统一权威的国家标准工作机制。
- (2) 促进行业标准规范有序发展。
- (3) 促进产业应用与标准化的紧密互动。
- (4) 推动军民标准兼容。

### 二、加强标准体系建设

- (5) 科学构建标准体系。
  - (6) 优化完善各级标准。
  - (7) 推进急需重点标准制定。
-

---

### 三、提升标准质量和基础能力

- （**8**）提高标准适用性。
- （**9**）提高标准先进性。
- （**10**）提高标准制定的规范性。
- （**11**）加强标准化基础能力建设。

### 四、强化标准宣传实施

- （**12**）加强标准的宣传解读。
  - （**13**）加大标准实施力度。
-



---

## 五、加强国际标准化工作

（**14**）实质性参与国际标准化活动。

（**15**）推动国际标准化工作常态化、持续化。

## 六、抓好标准化人才队伍建设

（**16**）积极开展教育培训。

（**17**）引进和培育高端人才。

## 七、做好资金保障

（**18**）做好财政资金保障工作。

（**19**）鼓励社会资金支持。

---

- 
- 我们有了顶层设计的优秀文件
  - 内化于心，外化于行才能把好想法，通过好行动转化为好结果。
  - 提高意识，深化认识，拓广共识，网络信息安全才有牢固的基础。
-

- 
- 预祝我们的信息安全标准化工作从学习、借鉴阶段，跨越到结合国情，创造创新，中看中用的新阶段。
  - 历史把担当重任的使命交付给了我们年轻的战友们。
  - 我们老同志要继续发挥人梯和铺路石的作用。
  - 让我们真抓实干，开拓前进，展现我中华的智慧，增强我信息安全的能力。
-

---

谢谢

---