远程办公安全风险和标准化研究

姚相振

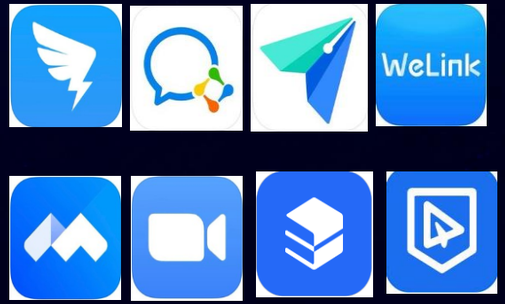
中国电子技术标准化研究院
信息安全中心副主任

远程办公应用背景

应用背景

- 远程办公，尤其是在线会议、即时通信、文档协作等典型远程办公应用场景，在疫情期间呈现了爆发式增长。2020年2月3号复工第一天，全国超过2亿人参与了远程办公，统计表明复工30天内远程办公需求环比上涨663%。

- 各类远程办公软件大量涌现，包括钉钉、企业微信、飞书、WeLink、腾讯会议、Zoom、金山文档、蓝信等，为远程办公活动的开展提供了便利的条件。



应用背景

- 远程办公应用的爆发式增长，在推动复工复产的同时，也带来了一系列安全问题。
  - ✓ Zoom安全事件。随着用户数量的激增，Zoom视频会议应用的安全漏洞被不断曝出，包括私自分享用户数据、会议信息ID可被收集导致信息泄露、虚假宣传的加密功能等严重安全风险，导致企业纷纷禁用Zoom。
  - ✓ 微盟删库事件。2月24日，微盟SaaS业务服务突然宕机，线上生产环境被破坏，大面积服务集群无法响应，上百万注册商户业务无法开展，核心业务停止近五天，三天内市值蒸发超过30亿。

远程办公安全风险

- **供应方安全风险。**
  - ✓ 提供远程办公系统的供应方安全能力参差不齐，部分供应方在安全开发运维、数据保护、个人信息保护等方面能力较弱，难以满足开展安全远程办公的要求。
- **远程办公系统自身安全风险。**
  - ✓ 在线会议、即时通信、文档协作等办公场景下系统安全功能不完备，系统自身的安全漏洞，不合适的安全配置等问题，将直接影响远程办公安全。
- **设备风险。**
  - ✓ 用于远程办公的设备，特别是用户自有设备，在接入远程办公系统时，由于未安装或及时更新安全防护软件，未启用适当的安全策略，被植入恶意软件等原因，可能将权限滥用、数据泄露等风险引入机构内部网络。

安全风险

- **数据安全风险。**
  - ✓ 远程办公场景中，通过远程办公系统可访问机构的数据，由于数据访问权限的不合理设置、远程办公系统自身的安全漏洞、用户不当操作等，可能导致机构数据泄漏。此外，由于远程办公系统基于云计算平台部署，机构可能失去对数据的直接管理和控制能力，存在数据被非授权访问和使用的风险。
- **个人信息保护风险。**
  - ✓ 远程办公系统的部分功能（例如，企业通信录、健康情况汇总、活动轨迹填报等），可能收集、存储用户的个人信息（例如，姓名、电话、位置信息、身份证件号码、生物特征识别数据等），存在被滥采、滥用和泄露的风险。

安全风险

- 网络通信风险。
  - ✓ 用户和远程办公系统通常利用公用网络进行通信，存在通信中断，通信数据被篡改、被窃听的风险。同时，远程办公系统可能遭受恶意攻击(例如，分布式拒绝服务攻击等)，导致办公活动难以进行。
- 环境风险。
  - ✓ 远程办公通常在居家环境或公共场所进行。居家环境中，由于家用网络设备安全防护能力和网络通信保障能力较弱，存在网络入侵和通信中断风险。公共场所中，由于网络环境和人员组成复杂，存在设备接入不安全网络、数据被窃取、设备丢失或被盗等风险。

安全风险

- 业务连续性风险。
  - ✓ 远程办公增加了使用方关键业务、高风险业务的安全风险，远程办公系统可能由于负载能力、访问控制措施、容灾备份、应急能力等方面的不足导致业务连续性风险。
- 人员风险。
  - ✓ 用户可能由于安全意识缺失或未严格遵守使用方的管理要求，引入安全风险，例如，将设备、账号与他人共享导致对使用方业务系统的恶意攻击；采用弱口令造成身份仿冒等。

远程办公安全标准

国外标准

NIST

- SP 800-46 Rev. 2 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
  - ✓ 从机构角度分析了VPN、远程桌面等典型远程办公场景的安全风险，并对强化各类远程办公场景安全性提出了建议。

- SP 800-114 Rev. 1 User's Guide to Telework and Bring Your Own Device (BYOD) Security
  - ✓ 从用户角度对用户使用VPN、远程桌面等方式开展远程办公提出了安全建议。

国外标准

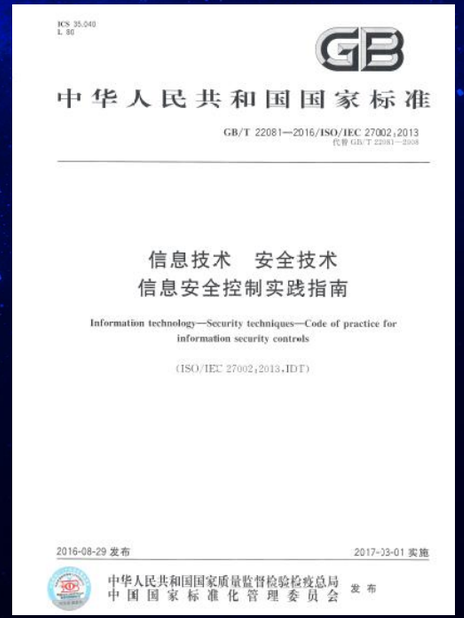
NIST

- SP 1800-21 (Draft) Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)
  - ✓ 针对移动设备的安全性问题，介绍了可以在组织网络环境中综合使用的各种移动安全技术。说明了如何通过标准的、商业化产品实现组织在移动设备安全和隐私方面的要求。
- SP 800-164 (Draft) Guidelines on Hardware-Rooted Security in Mobile Devices
  - ✓ 提供一个可在各种移动设备上实现的通用安全技术基线，帮助保护组织的移动设备以及在组织中使用的属于个人的设备。该安全技术基线着重于通过使用基于硬件的信任根来提供设备完整性、隔离性和存储保护的安全功能。

国外标准

ISO/IEC JTC1/SC27

- ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls (GB/T 22081:2016 信息技术 安全技术 信息安全控制实践指南)



ICS 35.040
L 80

GB

中华人民共和国国家标准

GB/T 22081—2016/ISO/IEC 27002:2013
代替 GB/T 22081—2008

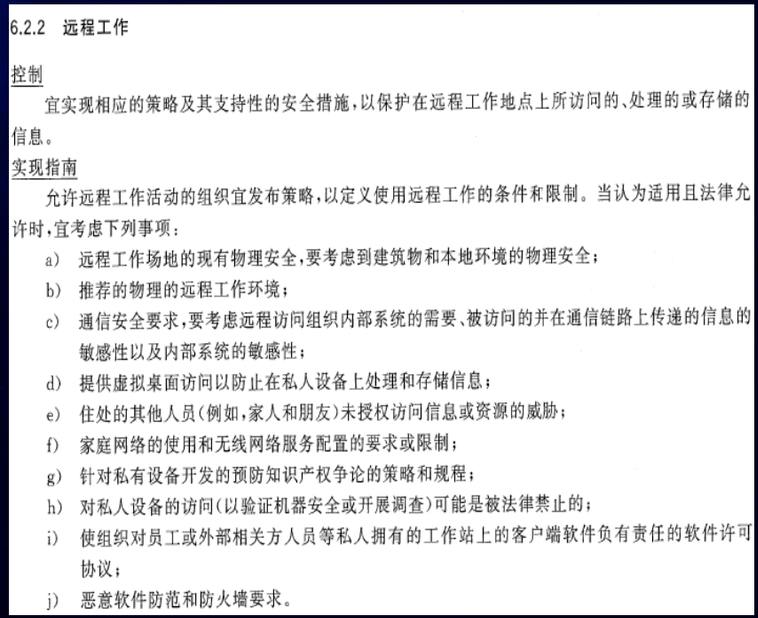
信息技术 安全技术
信息安全控制实践指南

Information technology—Security techniques—Code of practice for information security controls

(ISO/IEC 27002:2013,IDT)

2016-08-29 发布　　2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布



6.2.2 远程工作

控制

宜实现相应的策略及其支持性的安全措施，以保护在远程工作地点上所访问的、处理的或存储的信息。

实现指南

允许远程工作活动的组织宜发布策略，以定义使用远程工作的条件和限制。当认为适用且法律允许时，宜考虑下列事项：

a) 远程工作场地的现有物理安全，要考虑到建筑物和本地环境的物理安全；
b) 推荐的物理的远程工作环境；
c) 通信安全要求，要考虑远程访问组织内部系统的需要、被访问的并在通信链路上传递的信息的敏感性以及内部系统的敏感性；
d) 提供虚拟桌面访问以防止在私人设备上处理和存储信息；
e) 住处的其他人员（例如，家人和朋友）未授权访问信息或资源的威胁；
f) 家庭网络的使用和无线网络服务配置的要求或限制；
g) 针对私有设备开发的预防知识产权争论的策略和规程；
h) 对私人设备的访问（以验证机器安全或开展调查）可能是被法律禁止的；
i) 使组织对员工或外部相关方人员等私人拥有的工作站上的客户端软件负有责任的软件许可协议；
j) 恶意软件防范和防火墙要求。

国外标准

- 信安标委（编号SAC/TC260）成立于2002年4月，是国家标准化管理委员会直属标委会，业务上受中央网信办指导。
- 工作范围：包括信息安全技术、机制、服务、管理、评估等领域标准化工作。
- 工作职责：信安标委对网络安全国家标准进行统一技术归口，统一组织申报、送审和报批 （《关于加强国家网络安全标准化工作的若干意见》中网办发文[2016]5号）。
- 对口国际：ISO/IEC JTC1 SC27 （国际标准化组织国际电工委员会第一联合技术委员会信息安全分委员会）。
- 中国电子技术标准化研究院是信安标委秘书处所在单位。

国家标准—网络安全标准总体情况

截至2020年7月，委员会归口管理的已发布国家标准达313项，在研国家标准制修订项目74项，主要涉及密码、鉴别与授权、安全评估、通信安全、安全管理、大数据安全等领域。这些标准为国家网络安全审查、信息安全等级保护、信息安全产品检测与认证、信息安全风险评估、信息系统灾难恢复等国家网络安全保障工作，以及《网络安全法》 《电子签名法》《密码法》的实施等提供了强有力的标准化支撑。

相关国家标准

等级保护

国标号	标准名称
GB/T 22239-2019	信息安全技术 网络安全等级保护基本要求
GB/T 25070-2019	信息安全技术 网络安全等级保护安全设计技术要求
GB/T 28448-2019	信息安全技术 网络安全等级保护测评要求
GB/T 36627-2018	信息安全技术 网络安全等级保护测试评估技术指南
GB/T 28449-2018	信息安全技术 网络安全等级保护测评过程指南
GB/T 36958-2018	信息安全技术 网络安全等级保护安全管理中心技术要求
GB/T 36959-2018	信息安全技术 网络安全等级保护测评机构能力要求和评估规范
GB/T 22240-2020	信息安全技术 网络安全等级保护定级指南
GB/T 25058-2019	信息安全技术 网络安全等级保护实施指南

相关国家标准

办公信息系统和办公设备

国标号	标准名称
GB/T 37094—2018	信息安全技术 办公信息系统安全管理要求
GB/T 37095—2018	信息安全技术 办公信息系统安全基本技术要求
GB/T 37096—2018	信息安全技术 办公信息系统安全测试规范
GB/T 29244—2012	信息安全技术 办公设备基本安全要求
GB/T 38558—2020	信息安全技术 办公设备安全测试方法
GB/T 35282—2017	信息安全技术 电子政务移动办公系统安全技术规范
GB/T 37091—2018	信息安全技术 安全办公U盘安全技术要求

相关国家标准

智能终端

标准号	标准名称
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
GB/T 30284-2020	移动通信智能终端操作系统安全技术要求（EAL2级）
GB/T 32927-2016	信息安全技术 移动智能终端安全架构
GB/T 34975-2017	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
GB/T 34976-2017	信息安全技术 移动智能终端操作系统安全技术要求和测试评价方法

相关国家标准

云计算服务

标准号	标准名称
GB/T 31168—2014	信息安全技术 云计算服务安全能力要求
GB/T 31167—2014	信息安全技术 云计算服务安全指南
GB/T 34942—2017	信息安全技术 云计算服务安全能力评估方法
GB/T 37950—2019	信息安全技术 桌面云安全技术要求
GB/T 37956—2019	信息安全技术 网站安全云防护平台技术要求
GB/T 38249—2019	信息安全技术 政府网站云计算服务安全指南

网络安全实践指南

- 今年3月，安标委针对远程办公领域面临的安全风险，发布了《网络安全标准实践指南——远程办公安全防护》

- 实践指南分析了在线会议、即时通信、文档协作等典型远程办公应用场景中存在的主要安全风险，从安全管理、安全运维等方面，给出了具体的安全控制措施建议，为远程办公安全防护提供参考。


TC260-PG-20201A

网络安全标准实践指南

—远程办公安全防护

(v1.0-202003)

全国信息安全标准化技术委员会秘书处

2020 年 03 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

THANKS

全球网络安全 倾听北京声音